



Process Query Systems, LLC

16 Cavendish Court
Lebanon, NH 03766
+1.603.727.4477

support@flowtraq.com

FlowTraq Q4/13 User Manual

Process Query Systems, LLC

Publication date August, 2013

Copyright © 2009-2013 Process Query Systems, LLC

Table of Contents

1. Introduction	1
System Overview	1
Support, Training, and Professional Services	2
Technical Support	2
Training and Professional Services	3
Change Log	3
Changes in FlowTraq Q4/13	3
Changes in FlowTraq Q3/13	3
Changes in older versions of FlowTraq	4
2. Installation	5
System Requirements	5
Server Hardware Requirements	5
Client Hardware Requirements	7
Platform Requirements	7
Installation	7
Installation Overview	7
Installing or Upgrading FlowTraq Server	8
Installing FlowTraq Client	11
3. Initial Configuration	15
Launching FlowTraq Client	15
Logging In	15
Entering a License Key	17
User Administration	18
User Privileges	18
Changing Passwords	19
Adding and Removing Users	20
Granting and Revoking Administrative Privileges	21
User Access Control	21
4. FlowTraq User Interface	23
The Workspace	23
Filtering	24
View Selection	26
Time Navigation	29
Workspace Operations	31
5. FlowTraq Web Interface and FlowTraq NBI Server	34
Software Prerequisites	34
Installation Overview	34
Detailed Installation Guides	35
OpenSuSE Linux 11 - Installation Guide	35
Ubuntu Linux 10 (Lucid Lynx) - Installation Guide	38
CentOS 6.3 - Installation Guide	41
Access	44
Installation Troubleshooting	44
Error: NBI server not configured.	44
Error: NBI server authentication failed.	45
Error: The FlowTraq Server failed to identify itself.	45
Warning: The NBI server is not authenticated with this FlowTraq server.	45
6. Configuring Flow Sources	46
Supported Input Formats	46
Configuring NetFlow, cFlow, jFlow, IPFIX, and NSEL	47
Configuring sFlow	48

Using Flow Exporter	50
Troubleshooting Flow Sources	50
7. The Dashboard	54
Setting Up Your Dashboard	54
Pages	56
Managing Widgets	56
Widget Types	58
8. Interactive Reports (Workspaces)	61
Workspace Overview	61
Example Workspaces	62
Customizing Workspaces	62
Time Navigation	62
Filtering	63
Views	68
Workspace Details	72
Saving and Sharing Workspaces	73
Importing and Exporting Workspaces	73
Workspaces Widget	74
Printing and Saving Interactive Reports	74
9. Scheduled Reports	75
Scheduling Reports	75
Managing and Retrieving Reports	79
Editing, Disabling, and Deleted Scheduled Reports	79
Retrieving Reports	80
Deleting Generated Reports	80
10. Session Explorer	81
Accessing Session Explorer	81
Using Session Explorer	82
11. Alerts and Notifications	83
Setting Up Alerts	83
Managing and Retrieving Alerts	86
Editing, Disabling, and Deleting Alerts	86
Viewing Alert Causes	86
Alert Notifications	86
Notifications on the Dashboard	87
Notifications via E-mail	87
Notifications via Syslog Over UDP	88
Retrieving Notifications via the Command Line	89
12. Server Optimization and Administration	92
Performance Tuning	92
Performance Indicators	92
Performance Controls	93
Upgrading FlowTraq	96
Automatic Client Upgrades	96
Advanced Administration	98
Starting and Stopping FlowTraq Server	98
Backing Up the Session Database	99
Clearing the FlowTraq Session Database	100
The FlowTraq Server Configuration File: <code>flowtraq.conf</code>	100
13. Command Line Interface	108
Overview	108
Retrieving Raw Session Data from the Command Line with <code>ftsq</code>	108
Time Navigation	111
Filter String Syntax	112

Retrieving Statistical Queries from the Command Line with ftstat	114
Managing Users from the Command Line with ftum	116
Session Key Reauthentication	117
Retrieving Alert Notifications via the Command Line	118
14. The FlowTraq Network Behavioral Intelligence Toolkit	119
Overview	119
Configuration	120
Basic Parameters	120
Training Options	120
Logging Options	120
Usage Notes	121
ftbfg	121
ftdos	121
ftscan	123
fttcv	123
A. Enabling Flow Export on Common Devices	125
CISCO IOS	125
B. FlowProxy	127
Installing FlowProxy	127
Starting and Stopping FlowTraq Server	128
Windows	128
Mac OS X	128
Linux	128
BSD	129
Solaris	129
The FlowProxy Configuration File	129
Making Changes to flowproxy.conf	129
Configuration File Format	130
C. FlowTraq Web API Reference	131
Authentication	131
Request Parameters	131
Response Parameters	131
Example	131
Retrieving Processed FlowTraq Views	132
Request Parameters	132
Response Parameters	133
Example	133
Retrieving Raw NetFlow Sessions	133
Request Parameters	134
Response Parameters	134
Example	134
D. Flow FAQs	135
D. Legal Notices	137
END USER LICENSE AGREEMENT FOR FLOWTRAQ	137
Third-Party Software Components	148
Restlet	148
JFreeChart	149

Chapter 1. Introduction

Welcome to the FlowTraq user manual. This document contains in-depth information on installing, configuring, and effectively using the powerful and valuable features available in FlowTraq.

FlowTraq is a full-fidelity flow collector designed to combine the tasks of network monitoring, security, and forensics in one powerful, fast, and easy-to-use suite. In FlowTraq, you can view flow traffic from routers, managed switches, and other network devices.

FlowTraq was designed to flexibly meet the requirements of large enterprise, government, and small business in one product. Key features include:

- FlowTraq is compatible with all common network flow formats: NetFlow version 1, 5, 7, and 9; sFlow; cFlow; jFlow; IPFIX over TCP and UDP; and CISCO NSEL (ASA Firewall Events).
- FlowTraq is fully IPv6 capable.
- FlowTraq stores all the flow records it receives compactly and retrieves them with full fidelity. It never aggregates data and only discards the least-recent information in its database when the database becomes full, making years of full forensic recall feasible.
- FlowTraq provides the most powerful filtering technology in the industry, so you can quickly locate even small anomalies in the busy networks. See the section called “Filtering” for more information.
- FlowTraq help identify issues quickly with a configurable Dashboard. See Chapter 7, *The Dashboard* for more information.
- FlowTraq can generate alerts and send notifications via email, syslog over UDP, a command line interface, or the Dashboard. See Chapter 11, *Alerts and Notifications* for more information.
- FlowTraq can generate custom reports on a user-specified schedule. See Chapter 9, *Scheduled Reports* for more information.
- FlowTraq includes an extensive API and a full set of command line tools for scripting and web deployments. See Chapter 13, *Command Line Interface* for more information.
- FlowTraq has an interactive query mode specifically designed to help you get a handle on your network or perform forensic investigation after an incident. See Chapter 8, *Interactive Reports (Workspaces)* for more information.
- FlowTraq includes Flow Exporter, a software agent for sniffing a network interface and generating NetFlow. See the section called “Using Flow Exporter” for more information.
- FlowTraq can export results in a variety of standard formats, including PDF for printing and CSV for further processing.
- FlowTraq can be deployed in the datacenter, in the cloud, or on the workstation at your desk. Whether you are monitoring your network border, or are securing your key servers, FlowTraq will collect and store flow records of your network traffic.

This user manual was designed to help you get the best possible value out of your FlowTraq installation.

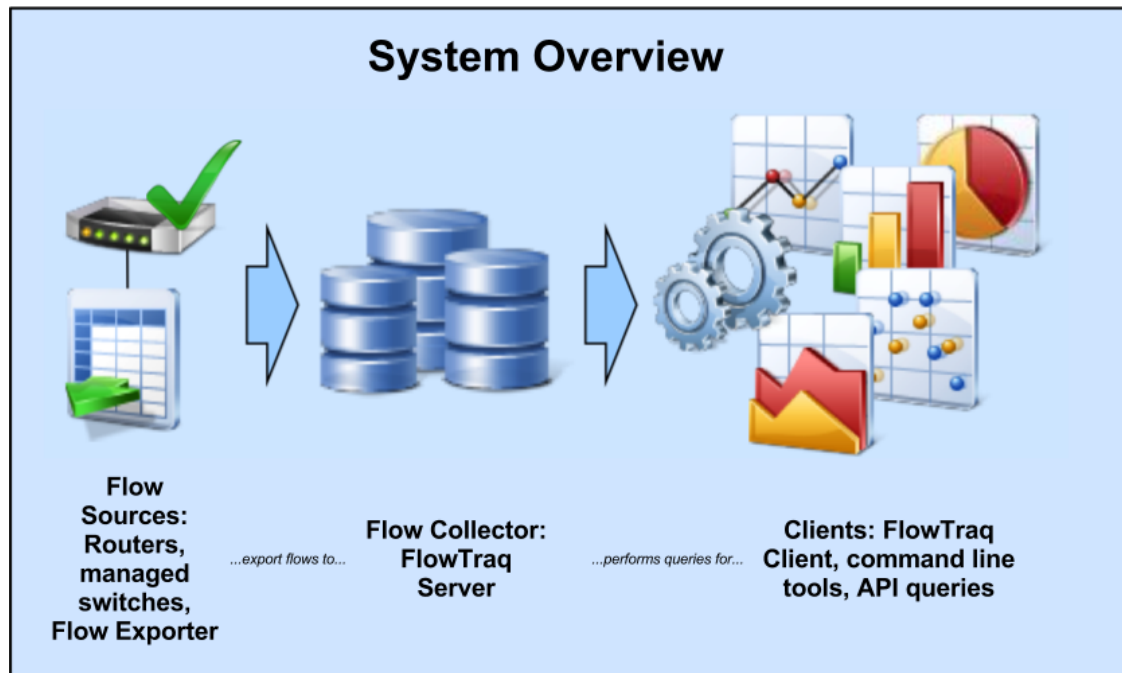
System Overview

A FlowTraq installation consists of an instance of FlowTraq Server and one or more instances of FlowTraq Client. Because FlowTraq is a networked application, you can access the system from anywhere on your network.

You can deploy FlowTraq Server on a dedicated server, on your own workstation, in a virtual machine, or in the cloud. In each case, FlowTraq will perform well as long as the server's hardware is sufficient to keep up with the network. (See the section called “System Requirements” for more information on hardware requirements.)

FlowTraq Server collects and stores the flows from your switches, routers, and other networked devices, and accepts connections from FlowTraq Client and the command line interface (CLI) tools. The client software and the CLI tools are used to analyze the collected flow records.

Figure 1.1. FlowTraq System Overview



Flows are exported by switches, routers, and other networked devices, the capabilities of which vary by manufacturer. Check with your network equipment vendors to see whether your devices are capable of exporting any of the FlowTraq compatible flow formats.

FlowTraq Client and the CLI tools use TCP/IP (TCP port 9640) to communicate with FlowTraq Server, and both the Client and the CLI tools are relatively lightweight. FlowTraq Client offers a user-configurable dashboard with many alerting and reporting options, and is designed for fast, interactive traffic analysis. The CLI tools offer the same analytic abilities as FlowTraq Client software; however, they are better suited for scripting and integration with third-party applications.

Support, Training, and Professional Services

We are happy to provide technical support, product training, and professional services to help you get started with FlowTraq or to help you make the most out of your FlowTraq deployment.

Technical Support

If can't find the answer to your question in this user manual, please check our support site:

<http://support.flowtraq.com>

Our support site contains a Knowledge Base of useful articles related to FlowTraq use, as well as a Q&A section.

If you still require assistance, please feel free to contact our support team at the points listed below:

Email support@flowtraq.com

Telephone (603) 727-4477 (9am-5pm Eastern Time)

Training and Professional Services

We would be happy to provide hands-on training at your site or via telepresence. In addition, we have certified consultants available to assist you with the planning, installation, implementation, and deployment of FlowTraq.

To arrange for training or consultation, please contact our professional services team at the points listed below:

Email training@flowtraq.com

Telephone (603) 727-4477 (9am-5pm Eastern Time)

Change Log

This section is updated with each release of FlowTraq.

Changes in FlowTraq Q4/13

- Feature: Nested Traffic Groups were added for fine-grained classification of traffic upon ingress
- Feature: CISCO NBAR and NBAR2 support for application names
- Feature: Palo Alto AppID support for application names
- Feature: Drag-to-zoom was added to workspace graphs
- Feature: Support for 32-bit IFindex numbers for interfaces
- Feature: Main dashboard graph can now be customized
- Feature: Users can store links to favorite workspaces on the dashboard
- Feature: New views include source port, destination port, and application views
- Lateral: Improved I/O scheduling for systems under extreme loads

Changes in FlowTraq Q3/13

- Feature: Traffic Groups were added for classification of traffic upon ingress.
- Feature: FriendlyNames for users allowing tagging of FlowTraq entities such as IP, Traffic Group, VLAN, Exporter, and Interface. Full list of ASN names included.
- Feature: New Views: CIDR block (using masklengths from export packet or ASN resolver), CIDR pairs, Exporter-Interface, Exporter-Interface pairs, Traffic Groups, and Traffic Group pairs (Web Interface only)
- Feature: Click-to-Filter and Click-to-Name on the Web Interface

- Feature: CLI environment variables for common parameters: FLOWTRAQ_USERNAME, FLOWTRAQ_PASSWORD, FLOWTRAQ_SERVER, FLOWTRAQ_PORT
- Feature: NBI alerted entities are now the default Web Dashboard view. Click-to-investigate was added to all alerts for improved workflow.
- Feature: Expanded API for external links to FlowTraq Web
- Feature: Server Administration page for the Web Interface for managing license keys and performance parameters.
- Feature: Updated Web Interface workspace now includes country, and ASN information for IP address and NetBlock views
- Lateral: Improved I/O handling on Linux systems
- Lateral: sFlow: configuration option to use 'agent address' instead of 'from' address as flow source
- Lateral: NBI tools are memory-bounded to 32MB per instance
- Lateral: Simplified database sizing for manual configuration and Web Interface
- Lateral: Reduced workload for NBI Blacklist and Behavioral Fingerprint Generator tools
- Lateral: Improved SIEM compatibility
- Lateral: Moved from hexadecimal to decimal representation of QoS

Changes in older versions of FlowTraq

For details on pre-Q3/13 versions of FlowTraq please contact your FlowTraq Support Representative.

Chapter 2. Installation

As described in Chapter 1, *Introduction*, FlowTraq is a client/server system where FlowTraq Server collects and analyzes flow records, and one or more instances of FlowTraq Client can connect to FlowTraq Server to retrieve the data.

This chapter describes FlowTraq's requirements and installation procedures.

System Requirements

Server Hardware Requirements

FlowTraq's hardware requirements depend heavily on the number of devices sending NetFlow information to it, and the amount and nature of traffic handled by those devices.

In order to provide full forensic recall capability, FlowTraq stores every flow record it receives to disk indefinitely, as long as there is room in the database. In addition to storing flow records on disk, FlowTraq Server keeps a memory cache of recently received records. The larger this cache, the larger the number of records which can be accessed quickly.

This full-fidelity feature allows for more powerful analysis and forensic capabilities than traditional flow collectors. However, it also means that FlowTraq can be more demanding of the hardware it's running on than traditional flow collectors.

Many customers opt to purchase hardware specifically for their FlowTraq installation. The table below gives some rules of thumb for configuring a hardware platform for FlowTraq Server:

Table 2.1. FlowTraq Server Hardware Configuration Guidelines

Flow Rate	CPU Examples	RAM	Disk
up to 4 million/hr	Core-2, i5, Athlon II-X4, 2Ghz	4GB-8GB (DDR3-1066)	Single disk at 5,400 rpm
up to 20 million/hr	i7-950, Phenom II-X6, 2.5Ghz	8GB-24GB (DDR3-1066)	Single or 3-disk RAID, 7,200 rpm
up to 100 million/hr	Xeon Nehalem W5590, Opteron 6174, 3Ghz	24GB-128GB (DDR-1333)	3-disk RAID, 10Krpm
more than 100 million/hr	Contact us...	Contact us...	Contact us...

The preceding configurations should be interpreted as guidelines. To determine your requirements, test the software's performance in your network environment.

Every network environment is different, and every organization's reporting needs and alerting needs are unique to the organization. You may be able to get the job done with less powerful hardware. A older processor such as a Core 2 Duo may still be able to handle the same input flow rate as a Xeon Nehalem W5590; however, queries may take longer to service than they would on the faster CPU.

Tip

In extremely demanding environments (such as those with a high flow load, many FlowTraq users, or heavy Alert usage), you may wish to run more than one FlowTraq instance and divide

the workload among them. For instance, you might set up two instances of FlowTraq Server, and have half of your flow sources report to the first and the other half report to the second.



Caution: 32-bit environments

Although FlowTraq will work in a 32-bit environment, we strongly recommend that FlowTraq Server be installed on a 64-bit (x86-64) platform.

On 32-bit platforms, FlowTraq Server will only be able to allocate approximately 2GB of RAM for its memory cache. This is unlikely to be sufficient in most environments.

Using a 64-bit operating system will allow FlowTraq Server software to allocate more RAM, which allows for a longer instant recall history and a higher input flow rate.

Note that in order to be able to take advantage of a 64-bit platform, both the CPU *and* the operating system must be 64-bit.

Frequently Asked Questions

1. How many cores do I need?

If your choice is between more cores at a lower clock frequency, or fewer cores at a higher clock frequency, we recommend you go with the latter. A higher clock frequency helps individual threads run faster, while having additional cores allows more threads to run concurrently. FlowTraq Server does benefit from having additional cores because it is heavily multi-threaded; however, we have found that a higher clock speed gives a quicker response to client requests.

A general rule of thumb is that 4 cores are more than enough for most installations. In certain cases we would recommend more than 4 cores. For example, if you plan to run many input ports, or if you plan to serve a large number of concurrently-connected clients, then might suggest 6, or more, cores.

2. All else being equal, should I choose a server with more RAM, or a server with faster RAM?

The more RAM, the better. More RAM means a longer history in the cache, which means fewer disk accesses. Disk is very slow compared to RAM, so the more data FlowTraq Server can keep in RAM, the quicker the queries return, and the faster your interactive traffic analysis will be.

3. How much disk space do I need for my flow database?

The answer to this question depends on your flow rate and on how many months or years of historical forensic data you need to keep.

Flow data is very compact compared to packet captures. A rule of thumb we have observed is that a typical end user generates 100MB of stored flow records per year. So if there are 1000 end users in your network environment, and you need to be able to retain forensic records for 10 years, make sure you have at least $100\text{MB}/\text{user}/\text{year} * 1000 \text{ users} * 10 \text{ years} = 1,000,000\text{M}$ or 1TB of disk space.

You can dedicate up to 16TB of disk space to the database.

4. How fast a disk do I need?

The higher the RPMs, the better. Speed limitations in modern hard disks are caused by the time it takes for the disk to rotate and the desired data to appear under the heads. The faster the disk spins, the quicker data can be written and read back. If you can get 15K RPM or better, get it!

5. RAID or non-RAID?

A Redundant Array of Independent Disks is a beautiful thing when constructed correctly. But in many cases, RAID is slower than a single-disk setup. For instance, RAID levels 4, 5, and 6 offer great redundancy for a relatively small capacity overhead; however, each write will translate into as many as 4 physical disk accesses. Unless the disks are very fast, this may hurt more than it helps. RAID levels 0 (striping) and 1 (mirroring) generally offer faster read times at either a high capacity overhead (mirroring), or lack of redundancy (striping). We consider RAID 1+0 (striping and mirroring) ideal for speed, but it is expensive due to the capacity overhead.

Client Hardware Requirements

FlowTraq Client and the CLI (command-line interface) tools are lightweight and don't require a substantial hardware investment. FlowTraq Client is a Java application and will run on any system that supports the Sun Java 5 runtime (version 1.5) or newer. Most client systems will need no more than 1GB of RAM and a 1Ghz processor. Depending on your usage patterns, however, you may want to give the client system more RAM. 4GB RAM should be sufficient for even the heaviest FlowTraq Client users.

The FlowTraq Command Line Interface (CLI) tools are even more lightweight than FlowTraq Client, and will run on any system that supports TCP/IP networking.

Platform Requirements

FlowTraq Client	FlowTraq Client supports Windows XP, 2003, Vista, 2008, and 7 (x86 and x86-64 architectures); Mac OS X (10.5+, x86 and x86-64 architectures); Linux (Kernel 2.6+, x86 and x86-64 architectures); Solaris 10 (SPARC and x86-64 architectures); and FreeBSD.
-----------------	--

A Java Runtime Environment (JRE) version 1.5+, provided by Sun Microsystems/Oracle is required.



Caution

Please note that other JREs, including OpenJDK, are not supported.

FlowTraq Server	FlowTraq Server supports Windows XP, 2003, Vista, 2008, and 7 (x86 and x86-64 architectures); Mac OS X (10.5+, x86 and x86-64 architectures); Linux (Kernel 2.6+, x86 and x86-64 architectures); Solaris 10 (SPARC and x86-64 architectures); and FreeBSD.
-----------------	--

Installation

Installation Overview

Installing FlowTraq is a three-step process.

1. Install FlowTraq Server.
2. Install FlowTraq Client.
3. Configure FlowTraq and all flow sources.

The following sections outline steps 1 and 2 on each supported platform; step 3 is covered in the next two chapters.

Installing or Upgrading FlowTraq Server

Preparing For Installation

Before installing FlowTraq Server, please note the following:



Important

On busy networks or when collecting from a large number of exporters, FlowTraq Server can put a heavy load on a system. We strongly recommend installing FlowTraq on a dedicated server.



Caution

If you are upgrading an existing FlowTraq Server installation, the installer will shut down FlowTraq Server, install the new version, and restart FlowTraq Server. *During the upgrade process, no flows will be recorded.*



Tip

FlowTraq Server will not be able to collect any flow data if another flow collector is running on the same system because it will be unable to bind the required listen ports. Please remove or disable any other flow collector software before installing FlowTraq.



Tip

Many operating systems have host-based firewalls configured by default to block inbound traffic on frequently-used flow listen ports. FlowTraq Server's default listen ports UDP/2055 (NetFlow/IPFIX over UDP), UDP/9666 and UDP/9996 (cFlow/jFlow), UDP/6343 (sFlow), and TCP/9640 (FlowTraq Client connections). Please ensure traffic on these, and any other ports on which you will configure flow collection, can reach the machine running FlowTraq Server.

Windows

On the Windows platform, FlowTraq Server is distributed as a self-extracting installer.



Important

You must be logged in as an administrator to install or upgrade FlowTraq Server.

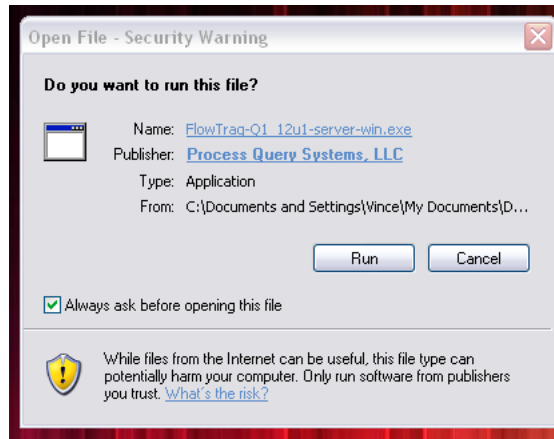
1. Download the installer from the FlowTraq download site.
2. Double-click the file to launch the installer, then follow the on-screen instructions to complete the installation process.



Tip

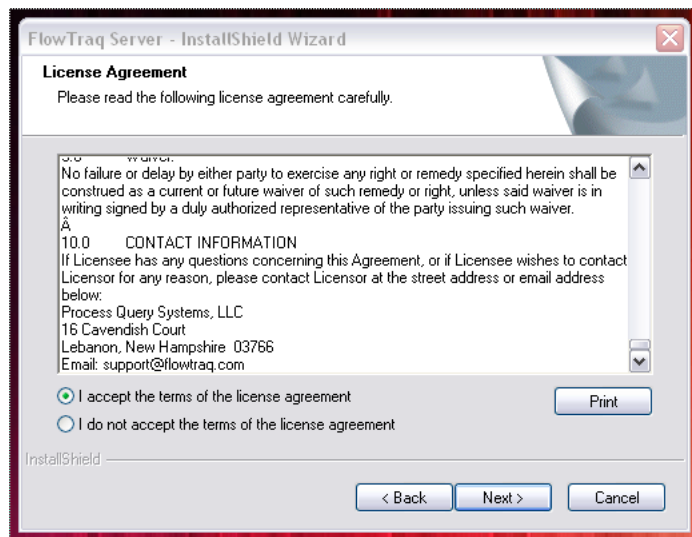
The installer is digitally signed by Process Query Systems, LLC. A warning similar to this one may appear when launching the installer from Internet Explorer. Click "Run" to continue with the installation.

Figure 2.1. Windows Installation Security Warning

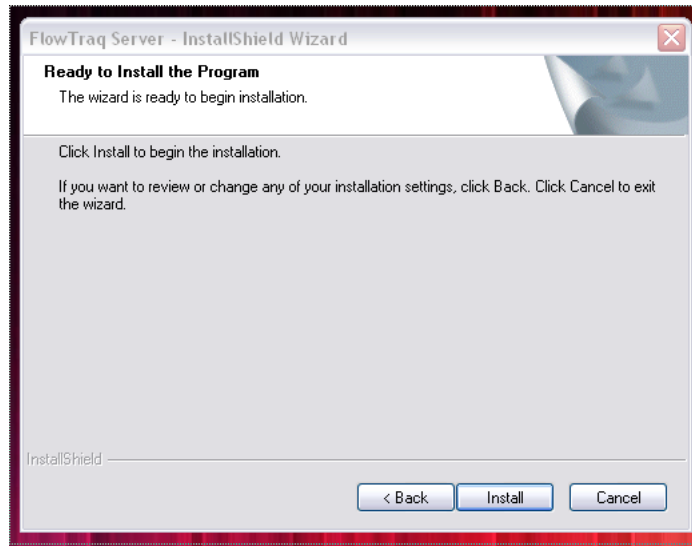


3. Review the license agreement and click the radio button to indicate your acceptance, then click "Next".

Figure 2.2. Windows End-User License Agreement



4. Click "Install" to install FlowTraq Server.

Figure 2.3. Windows Installation

Unix (including Mac OS X)

On Unix platforms (including Mac OS X), FlowTraQ Server is installed with a universal install script that detects your platform and selects and installs a compatible binary and startup scripts for your platform. The following Unix platforms are supported:

Table 2.2. FlowTraQ Unix Server Platform Support

Platform	Architecture	Startup Method
Debian Linux, Ubuntu Linux, and variants	32-bit Intel (x86), 64-bit Intel (x86-64)	Using <code>/etc/init.d</code> and <code>/etc/rc*</code>
RedHat Linux, CentOS, and variants	32-bit Intel (x86), 64-bit Intel (x86-64)	Using the <code>chkconfig</code> system
SUSE Linux, OpenSUSE and variants	32-bit Intel (x86), 64-bit Intel (x86-64)	Using <code>/etc/sbin/rc*</code>
Solaris	64-bit SPARC, 64-bit Intel (x86-64)	Using SVC manifests
FreeBSD	32-bit, 64-bit Intel (x86-64)	Using <code>/etc/rc.d</code>
Mac OS X	64-bit Intel (x86-64)	Using <code>launchd</code>

To install FlowTraQ Server, take the following steps.

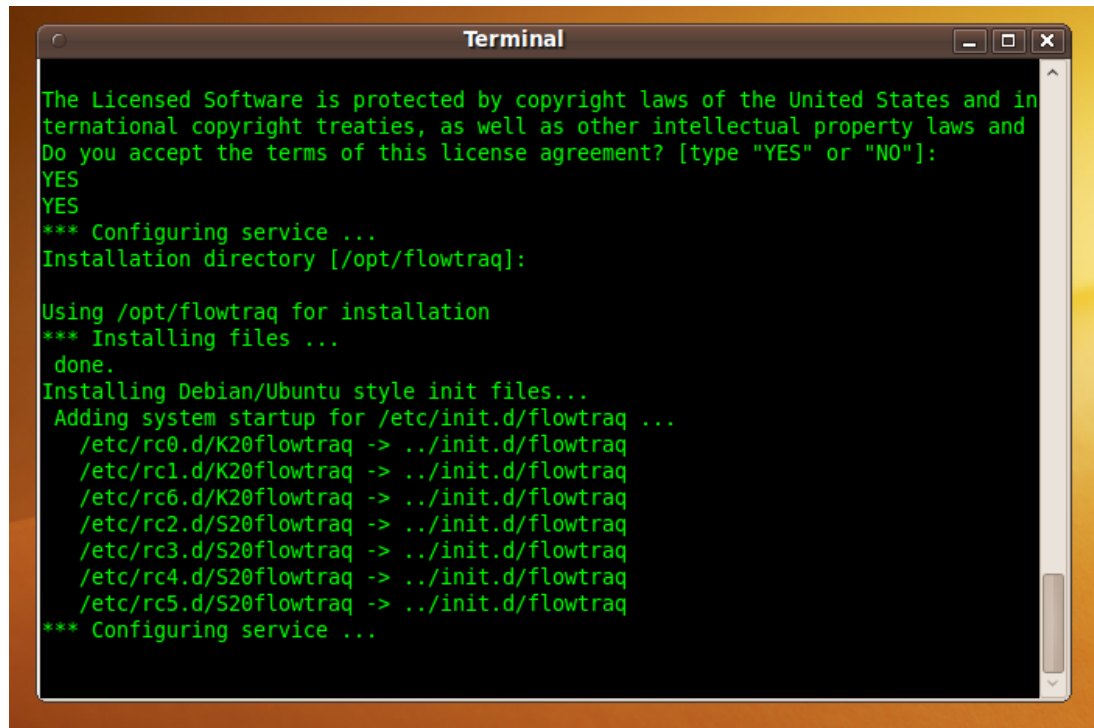
1. Download the universal Unix installer (`FlowTraQ-QX_XX-PLATFORM-server.sh.gz`, where `QX_XX` represents the current version of FlowTraQ).
2. Unzip the installer:


```
$ gunzip FlowTraQ-QX_XX-PLATFORM-server.sh.gz
```

 This produces `FlowTraQ-QX_XX-PLATFORM-server.sh`.
3. Run the installer with superuser privileges, either by running as root or via `sudo`:

```
$ sudo sh FlowTraq-QX_XX-PLATFORM-server.sh
```

Figure 2.4. Unix Installation



```
Terminal
The Licensed Software is protected by copyright laws of the United States and in
ternational copyright treaties, as well as other intellectual property laws and
Do you accept the terms of this license agreement? [type "YES" or "NO"]:
YES
YES
*** Configuring service ...
Installation directory [/opt/flowtraq]:

Using /opt/flowtraq for installation
*** Installing files ...
done.
Installing Debian/Ubuntu style init files...
Adding system startup for /etc/init.d/flowtraq ...
/etc/rc0.d/K20flowtraq -> ../init.d/flowtraq
/etc/rc1.d/K20flowtraq -> ../init.d/flowtraq
/etc/rc6.d/K20flowtraq -> ../init.d/flowtraq
/etc/rc2.d/S20flowtraq -> ../init.d/flowtraq
/etc/rc3.d/S20flowtraq -> ../init.d/flowtraq
/etc/rc4.d/S20flowtraq -> ../init.d/flowtraq
/etc/rc5.d/S20flowtraq -> ../init.d/flowtraq
*** Configuring service ...
```

4. Press [SPACE] to page through the license agreement, and type YES when prompted to indicate your acceptance.
5. If this is a new installation, you will be asked to select the installation directory. You can press [ENTER] to accept the default installation directory, or you can specify your own.



Important

The permissions on the installation directory needs allow the `flowtraq` process to write to the directory, as it will update various items at runtime.

If you are upgrading an existing FlowTraq Server installation, the current configuration is retained and the new server daemon is started right away.

Installing FlowTraq Client

Preparing For Installation

Before installing FlowTraq Client, please note the following:



Caution

FlowTraq Client requires a Java Runtime Environment (JRE), version 1.5+, provided by Sun Microsystems/Oracle. If you do not have a compatible Java Runtime Environment installed, please visit <http://java.com/> to download and install a compatible JRE before proceeding.

Windows

On the Windows platform, FlowTraq Client is distributed as a self-extracting installer.

Install FlowTraq Client by taking the following steps.

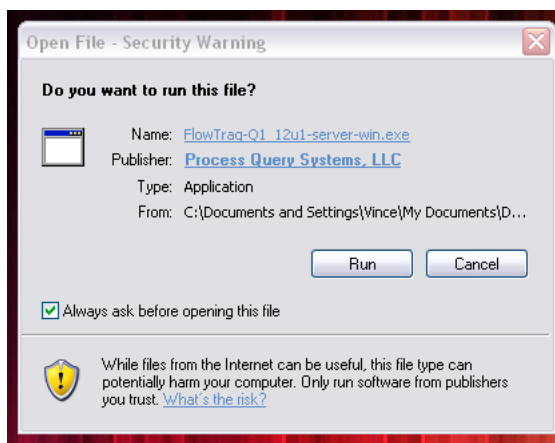
1. Download the installer from the FlowTraq download site.
2. Double-click the file to launch the installer, then follow the on-screen instructions to complete the installation process.



Important

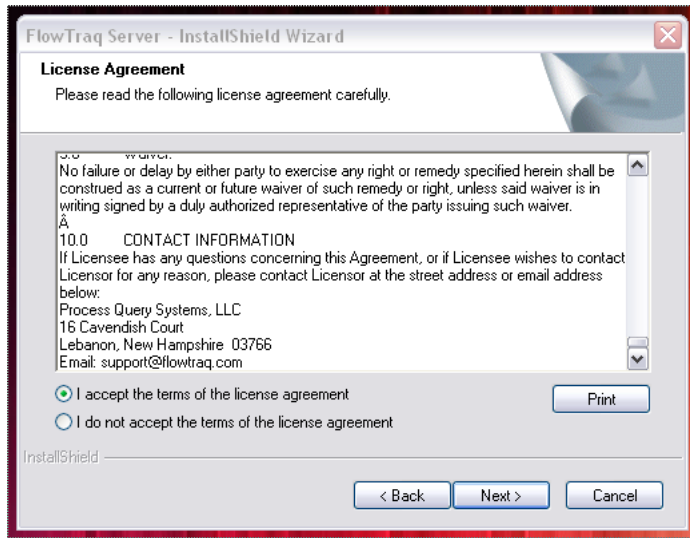
The installer is digitally signed by Process Query Systems, LLC. A warning similar to this one may appear when launching the installer from Internet Explorer. Click "Run" to continue with the installation.

Figure 2.5. Windows Installation Security Warning



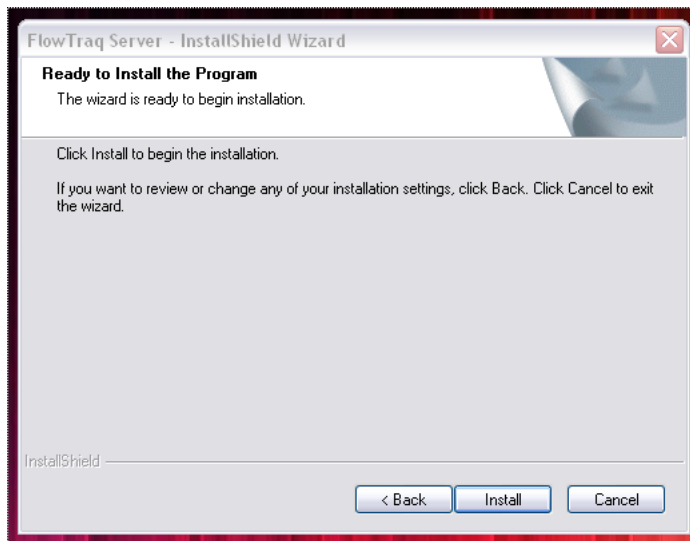
3. Review the license agreement and click the radio button to indicate your acceptance, then click "Next".

Figure 2.6. Windows End-User License Agreement



4. Click "Install" to install FlowTraQ Client.

Figure 2.7. Windows Installation



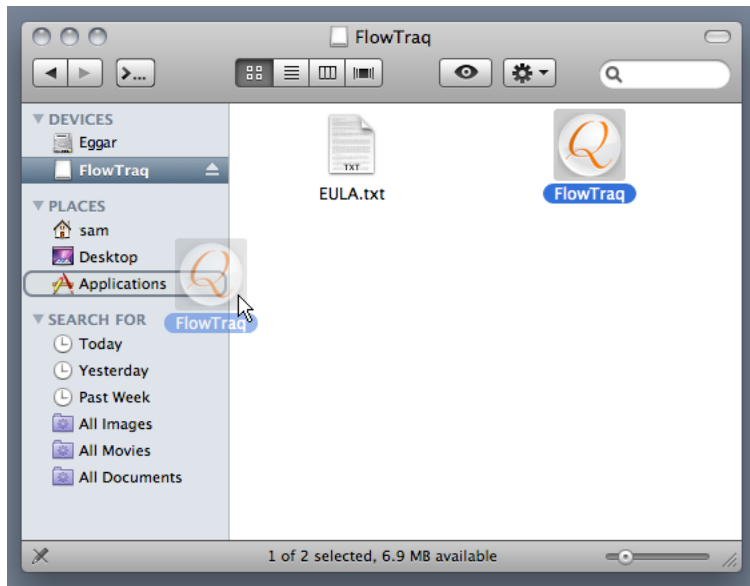
5. Launch FlowTraQ Client from the Start Menu.

Mac OS X

On Mac OS X, FlowTraQ Client is distributed as a mountable DMG disk image containing the application.

1. Download the DMG file.
2. Double-click the file to mount it.
3. Drag the application from the DMG to your Applications folder, or to a folder of your choosing.

Figure 2.8. Mac OS X Client Installation



4. Launch FlowTraq Client by double-clicking the application icon.

Unix

On Unix platforms, FlowTraq Client is installed with a universal install script that installs client libraries and startup scripts, similarly to FlowTraq Server. The Unix platforms supported by FlowTraq Client are the same as those supported by FlowTraq Server.

To install FlowTraq Client, take the following steps.

1. Download the universal Unix installer (`FlowTraq-QX_XX-PLATFORM.sh.gz` , where QX_XX represents the current version of FlowTraq).

2. Unzip the installer:

```
$ gunzip FlowTraq-QX_XX-PLATFORM.sh.gz
```

This produces `FlowTraq-QX_XX-PLATFORM.sh` .

3. Run the installer with superuser privileges, either by running as root or via `sudo` :

```
$ sudo sh FlowTraq-QX_XX-PLATFORM.sh
```

4. Press [SPACE] to page through the license agreement, and type YES when prompted to indicate your acceptance.
5. You will be asked to select the installation directory. You can press [ENTER] to accept the default installation directory, or you can specify your own.
6. A link to the startup script will be placed in `/usr/local/bin` . If your path contains that directory, you can launch FlowTraq Client by invoking the `flowtraq-client` . Otherwise, invoke `/usr/local/bin/flowtraq-client`.

Chapter 3. Initial Configuration

After installing FlowTraq, it is important to take a few administrative steps:

- Launch FlowTraq Client and log in for the first time.
- Install a license key.
- Perform some basic user management, including changing the default administrator password and creating a new user for day-to-day use.

These steps are outlined in this chapter.

Launching FlowTraq Client

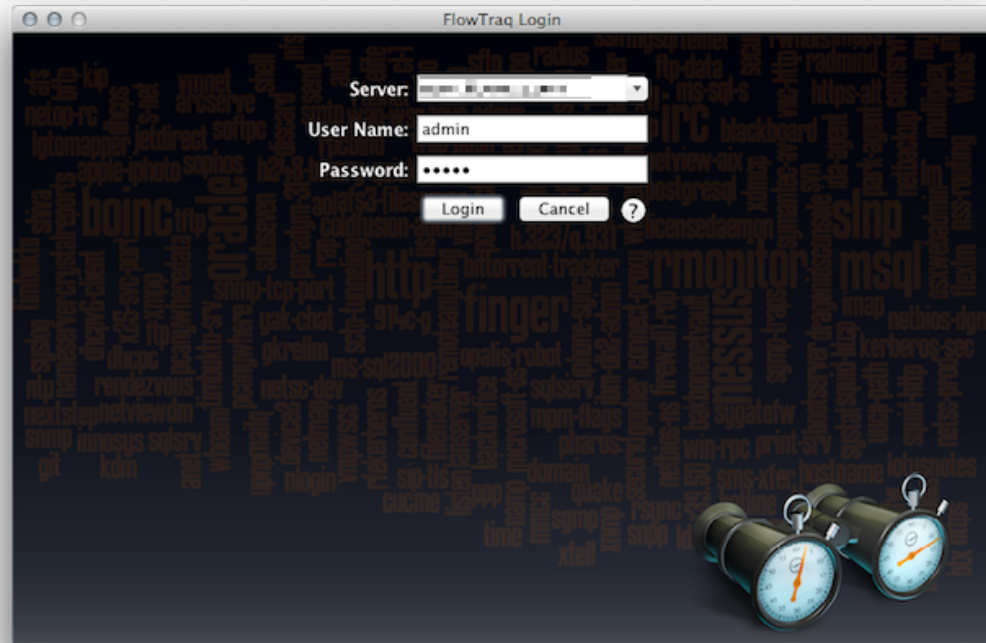
Launching FlowTraq Client is different on every platform.

Windows	Launch FlowTraq Client from the Start Menu.
Mac OS X	Launch FlowTraq Client by double-clicking the application icon in the <code>/Applications</code> folder (or the location you previously installed FlowTraq Client).
Other Unix platforms	Launch FlowTraq Client by invoking the <code>flowtraq-client</code> command from a Terminal. If <code>/usr/local/bin</code> is not in your path, add it to your path; otherwise, invoke <code>/usr/local/bin/flowtraq-client</code> .

Logging In

Upon launching FlowTraq Client, the first screen you'll see is the login window, which should look similar to this:

Figure 3.1. FlowTraq Login Window



In the **Server** field, enter the IP address or hostname of your server. If you are running FlowTraq Client on the same machine as FlowTraq Server, enter `localhost`.

Important

On a newly-installed FlowTraq instance, the default username and password is as follows:

Table 3.1. Default Username and Password

username	admin
password	admin

Please be sure to change the default administrator password to something more secure after you first log in (see the section called “Changing Passwords” for more information on how to do this).

FlowTraq Listen Port: TCP/9640

FlowTraQ Server listens for Client connections on TCP/9640 by default. Please ensure that systems running FlowTraQ Client can reach the machine running FlowTraQ Server on that port.

You can configure FlowTraq Server to listen on a different port number than the default 9640 by using the `listenport` directive in the FlowTraq configuration file. (Please see the section called “The FlowTraq Server Configuration File: `flowtraq.conf`” for more information on the FlowTraq configuration file.)

If you do so, in the login window, specify the port to connect to by adding a colon and the new port at the end of your IP address or hostname. Furthermore, if you are connecting over IPv6, please put the IPv6 address of your FlowTraq Server between square brackets, to ensure that the port specification is not confused with part of the IPv6 address. For example:

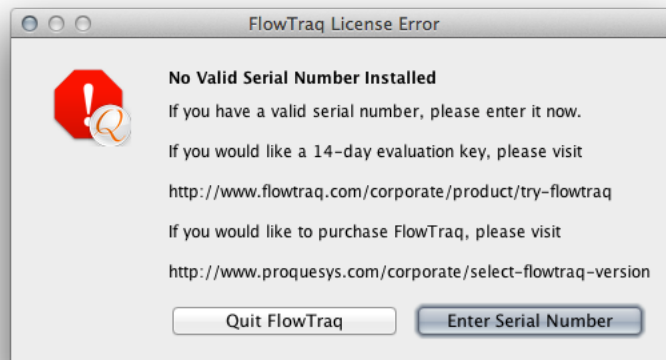
Table 3.2. Connecting to FlowTraq Server via IPv6

nitrogen:9641	log in to host nitrogen, which is listening on port TCP/9641
[fed9::c0:ffee]:9641	log in to IPv6 address fed9::c0:ffee, which is listening on port TCP/9641
192.168.0.150	log in to IPv4 address 192.168.0.150, which is listening on default port TCP/9640

Entering a License Key

Upon logging in for the first time, or, if you are using an evaluation license, when your evaluation period ends, you may receive the following prompt:

Figure 3.2. No Valid Serial Number installed



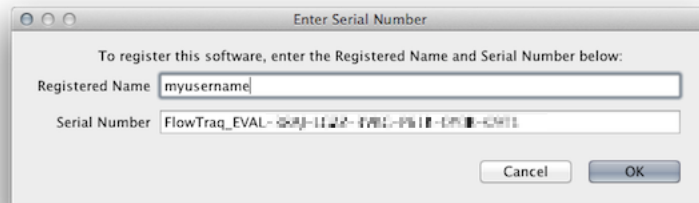
Click "Enter Serial Number" to enter a license key.



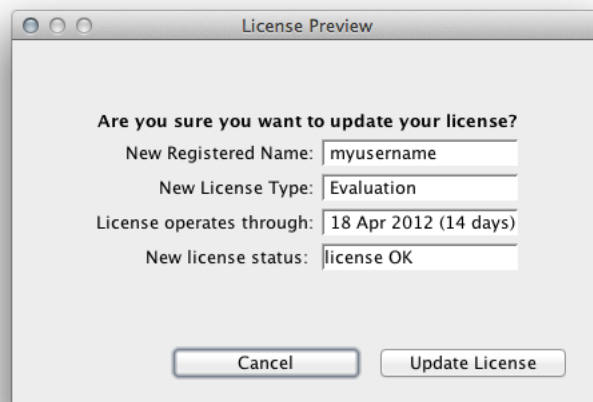
Important

If you do not have a current license key, please visit <http://www.flowtraq.com> or contact <sales@flowtraq.com> to purchase FlowTraq or to request an evaluation license.

Enter (or copy and paste) your license key and registered user name in the following window:

Figure 3.3. Enter License Key

Click "OK" to validate your license key:

Figure 3.4. License Preview

Confirm your license details, and if all looks well, click "Update License" to commit your changes.

The License Preference Panel

You can view your license details and update your license key in the same way with the License preference panel. Access it by clicking the "Preferences" button on Dashboard toolbar or selecting *Edit > Preferences...* from the Dashboard menu, and selecting the "License" tab.

User Administration

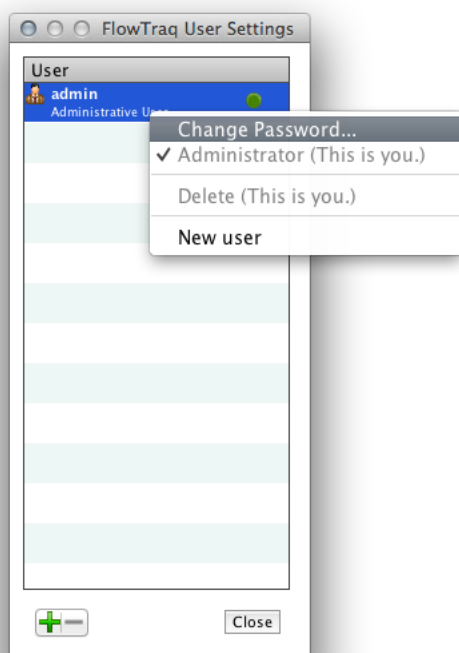
This section describes the different kinds of FlowTraq user accounts, and includes information on how to change user passwords, add and remove users, and grant and revoke privileges.

User Privileges

FlowTraq has two kinds of user accounts: *Administrative Users* or "Administrators" and *Unprivileged Users*.

Administrators (such as the default `admin` account) have access to the *User Settings* control panel:

Figure 3.5. User Settings Control Panel



- The green button indicates users that are currently logged in.
- Users with a blue jacket are unprivileged users.
- Users with a brown jacket are Administrators.

From this panel, an Administrator may add and remove user accounts, make other users into Administrative Users (or remove that status), and change user passwords.

Administrators can also set up access controls for each unprivileged user to restrict what sessions they can see when doing analytics. For more information on how to set up user access control, please see the section called “User Access Control”.



Important

Administrators also have access to the *License*, *Performance*, and *Memory* tabs of the Preferences Panel. These are described in The License Preference Panel and the section called “Performance Controls”.

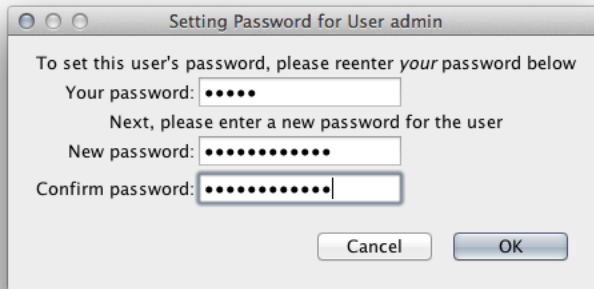
Upon first login, you should immediately change the password for `admin` and create a new user for day-to-day use.

Changing Passwords

You can change any user's password by taking the following steps:

1. Log in as an Administrator.
2. Open the *User Settings* control panel by selecting the *Users* button on the Dashboard toolbar the *Edit > User Accounts...* menu item.
3. Right-click a user and select the *Change Password...* menu item.

You will see a window similar to this one:



4. Enter your password, then enter the desired password for the new user twice, and click OK.

Changing Your Password as an Unprivileged User

Unprivileged users can change their own passwords by selecting *Edit > Change Password...* from the Dashboard menu.

Adding and Removing Users

You can add and remove users by taking the following steps:

1. Log in as an Administrator.
2. Open the *User Settings* control panel by selecting the *Users* button on the Dashboard toolbar the *Edit > User Accounts...* menu item.

To remove a user you may either:

- Right on the user and select *Delete*, OR
- Select the user and click the '-' button.

Important

You may not delete a user that is currently logged in. (This implies that you cannot delete yourself!)

To add a user, you may either:

- Right in the empty space at the end of the user list and select *New User*, OR
- Click the '+' button.

Then type a name for the new user and press [ENTER] .



User Name Rules

User names must conform to the following rules:

- Usernames must be between 2 and 32 characters.
- Usernames may contain spaces (but leading and trailing spaces are not counted).
- Usernames must NOT contain non UTF-8 characters.
- Usernames must NOT contain '@' or '|'.
- Usernames must NOT start with an underscore.

Finally, you will be prompted to set the new user's password.

Granting and Revoking Administrative Privileges

You can grant and revoke administrative privileges by taking the following steps:

1. Log in as an Administrator.
2. Open the *User Settings* control panel by selecting the *Users* button on the Dashboard toolbar the *Edit > User Accounts...* menu item.
3. Right-click the user whose privileges you wish to change.
 - If the user is not an administrator, select *Make administrator* to grant administrative privileges.
 - If the user is an administrator, there will be an item in the menu labeled "Administrator" with a check next to it. Select that item to revoke administrative privileges.



Important

You cannot revoke your own administrative privileges. (This is to prevent the system from getting into a state where there are no administrators.)

User Access Control

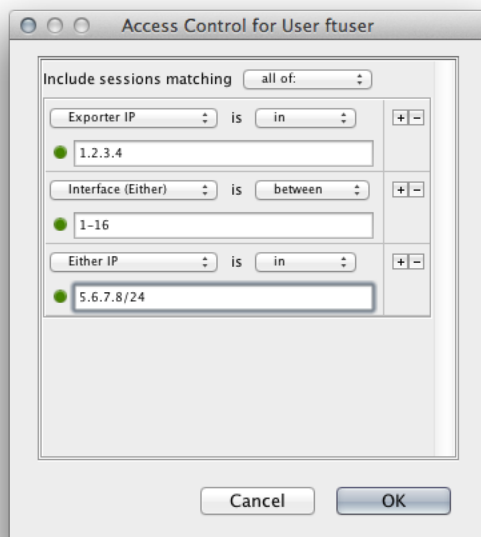
FlowTraq provides a fine-grained user access control mechanism which permits an administrator to decide which flows an unprivileged user may see. This is accomplished by setting a User Filter for each unprivileged user. When the unprivileged user logs in, he will only see sessions which match the User Filter. This is especially useful in multi-tenant/managed-services environments.

To set a user's User Filter, take the following steps:

1. Log in as an Administrator.
2. Open the *User Settings* control panel by selecting the *Users* button on the Dashboard toolbar the *Edit > User Accounts...* menu item.
3. Right-click the unprivileged user whose User Filter you wish to change and select "User Access Control..." (Note that setting a User Filter on an Administrator is not permitted.)

4. The User Access Control dialog appears:

Figure 3.6. User Access Control



5. Set the user's filter and click OK.

For more information on how to configure filters, please see the section called “Filtering”.



Important

Please note that unprivileged users can still see all Exporters in the Data Source Selection and Preferences Window. However, they will not see sessions from an exporter if they do not match their user filter; they will only know that an exporter exists and has sent flow records to FlowTraq.

Chapter 4. FlowTraq User Interface

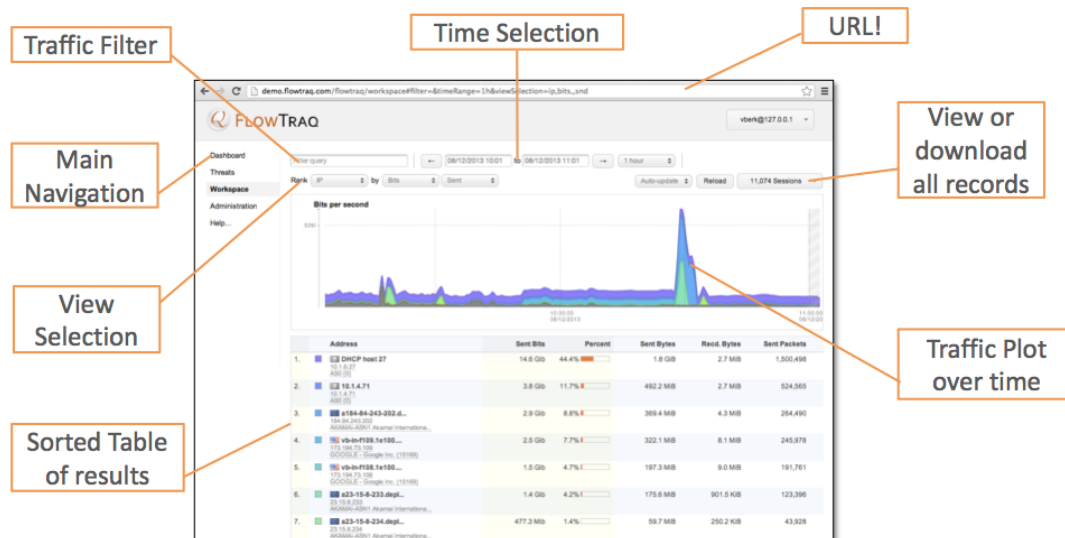
The default FlowTraq user interface is browser based and can be accessed by any Internet enabled device with a web browser. By default FlowTraq can be accessed through the */flowtraq* subdirectory on the server. For details on FlowTraq server installation, refer to the Installation Manual.

The Workspace

In FlowTraq the Workspace is your interactive analysis window into the traffic on your network. The Workspace features a powerful filtering interface that enables the analyst to select precisely the traffic of interest. Combined with hundreds of possible viewing combinations, the analyst can observe events on the network from any viewing angle, identifying patterns that remain hidden in traditional network analysis tools. By selecting objects the analyst can quickly pivot, zoom, and focus on suspicious activity, data breaches, and performance issues.

FlowTraq redefines traffic reporting by featuring a full-fidelity database that retains all flow records indefinitely. This means you can generate any view of your network, using any arbitrary filter, for any desired timeframe, whenever you need. With FlowTraq it is not necessary to define today what you want to analyze tomorrow, as all reports can be generated on the fly, post-hoc. Since all workspaces are defined in the URL, you can save interesting views of your traffic by bookmarking the URL. Additionally, since each view is generated dynamically, FlowTraq offers arbitrary zoom-in capability with full precision at any timescale.

Figure 4.1. Example Workspace



FlowTraq traffic navigation is defined by 3 key elements:

1. A *filter* selecting *what* traffic is to be ranked. The filter may define exporters, address ranges, protocols, etc.

Include sessions matching **all** of the following:

Client IP is not in 10.0.0.0/8, 192.168.0.0/16

TCP Flags are CWR ECN URG ACK PSH RST SYN FIN

[Add another filter...](#)

2. A *ranking view* selecting *how* traffic is to be ranked. Examples of rankings include top addresses by packet count, top exporters by update count, application by total connections, etc.

Rank **ASN** by **Unique...** **IP** **Total**

3. A *timeframe* selecting from *when to when* traffic is to be ranked. Timeframes can be specified in the absolute (date and time), or relative to now (last 3 hours).

← 08/12/2013 10:01 to 08/12/2013 11:01 → 1 hour

Filtering

Thanks to the full fidelity nature of the FlowTraq database every field of the session record can be filtered on. This includes derived fields such as country and autonomous system number, which are not found in the flow export records, and added by FlowTraq. Since FlowTraq re-assembles uni-directional flows back into bi-directional sessions, many filter options have both a *client* and a *server* side, such as ports, traffic groups, and byte/packet counts.

A filter selects which session records will be used to perform the ranking. This means that the filter is applied to each session record in the selected timeframe to decide if the record should be returned and included.



Important

Complex filters can be constructed by entering multiple values in a filter line, or by combining multiple filter lines:

When entering multiple values in a single filter line they are combined through a logical 'OR' operation, meaning they will use a *match any* approach.

Multiple filter lines can be combined through a *match all* (logical 'AND') or *match any* (logical 'OR') approach.

Address Block Filtering

FlowTraq filtering supports definitions of CIDR (classless interdomain routing) blocks in both IPv4 (32-bit addresses) and IPv6 (128-bit addresses). By using the 'slash-size' subnet mask notation, addresses in the entire range are matched. When specifying multiple CIDR blocks, the comma acts as a logical 'OR' in a positive match:

SRVIP==10.1.0.0/16 || SRVIP==10.2.0.0/16

Selecting 'not in' transforms the meaning to a logical 'AND' and negates the match:

SRVIP!=10.1.0.0/16 && SRVIP!=10.2.0.0/16

Client vs. Server vs. Either Behavior

FlowTraq supports matching specifically the 'client' or the 'server' side of a session for entities such as IP addresses, ports, autonomous systems, or interface index numbers. For example, this means the analyst can specifically choose to only select sessions where a particular address acts as a server (receiving the connection). When choosing 'either address', all sessions where either the server or the client address match the selected block will be included.



Important

When filtering on 'either' *only* matching entities are ranked.

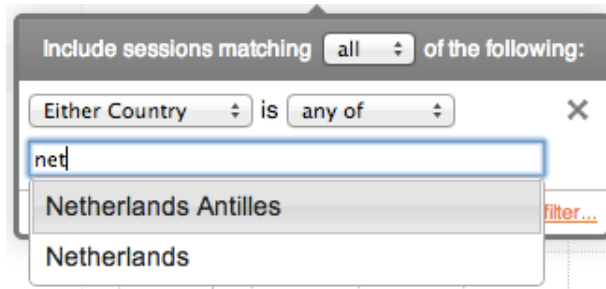
Example: either ASN = 32934 will only show FaceBook in the ASN-view, and FaceBook peers in the ASNPAIR-view.

When filtering on 'client' or 'server' side entities, *all entities* in the record are ranked.

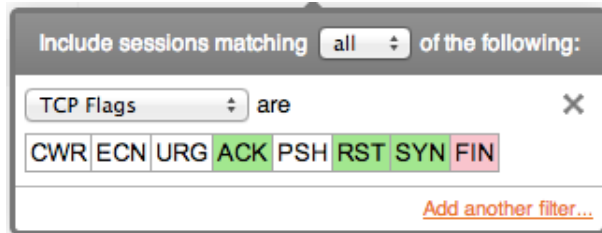
Example: SRVIP = 10.0.1.10 will only any IP that communicated with 10.0.1.10 (including the server itself) in an IP-view

Special Filters

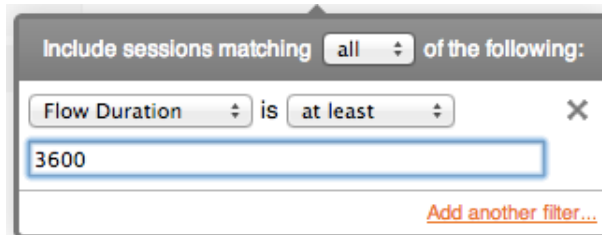
- Traffic groups and countries can only be filtered by their name. Simply start typing and they will auto-complete. Application name filtering is also performed by name, but does not support auto-complete.



- TCP flags are filtered by selecting which flags should be included (green), excluded (red), and don't-care (white). Click a flag multiple times to change the include/exclude status.

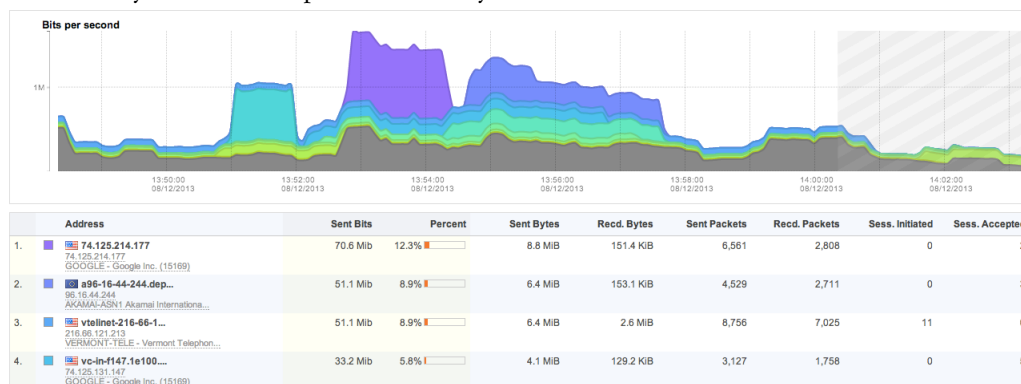


- Flow duration is computed from start and end times, and the filter is interpreted as duration in seconds. *However*: sessions are never longer than the value of the 'toolong' parameter (default is 8 hours maximum).



View Selection

FlowTraq supports a system where the analyst can create arbitrary top-N rankings for any entity found in the session record. A view is created by selecting which entity (such as IP address, netblock, ASN, ...) should be ranked based on what quantity (packets, bytes, connections, ...). Some selections allow the analyst to specify whether only sent, or only received quantities should be included. This example shows a workspace with *IP addresses* ranked by *bits sent*. The graph displays the progression of bits sent over time by each of the top IP addresses by color code:



The first column of the table shows the top IP addresses with their reverse-resolved name (if available), and the autonomous system in which the IP address resides. The ranking was performed on *bits sent* by each IP address. The percentage column displays the contribution of each entity for the total selected traffic based on the filter and current timeframe. The additional columns are auxiliary information and cannot be used for sorting.

Pair-wise Views

FlowTraq re-assembles uni-directional flows into bi-directional sessions, allowing some entities to be grouped in a pair-wise fashion. IP addresses, interface index numbers, VLAN identifiers, autonomous systems, traffic groups, and MAC addresses can all be ranked in pairwise views. The example image below shows total packets sent between the various FlowTraq office locations and the outside world based on the defined traffic groups:

	Traffic Group Pair		Total Packets	Percent
1.	 Bedford Colo (1)	↔ Centerra (2)	6,438,151	53.6% 
2.	 Outside World (0)	↔ Bedford Colo (1)	3,184,915	26.5% 
3.	 Outside World (0)	↔ Centerra (2)	1,034,655	8.6% 
4.	 Outside World (0)	↔ Nashua (3)	1,011,854	8.4% 
5.	 Bedford Colo (1)	↔ Bedford Colo (1)	336,647	2.8% 
6.	 Outside World (0)	↔ Outside World (0)	1,029	< 0.1% 
7.	 Centerra (2)	↔ Centerra (2)	459	< 0.1% 

Sent vs. Received vs. Total

Ranking of entities can be further controlled to only include bits/bytes/packets/sessions *sent*, or *received*. By default both sent and received counts are added into the ranking. By selecting 'sent' or 'received' the analyst is able to control the behavior of the ranking to include the selected count to or from each entity.



Important

Sent/Received differentiation is only available for entities that *CAN* be viewed in a pairwise fashion, although a pairwise view does not need to be selected. In other words, only entities that are present at each side of a communication (such as IP addresses, autonomous systems, traffic groups, ...) have a meaningful differentiation between bytes/bits/packets sent or received. When viewing accumulated TCP flags, for example, the directionality is meaningless as TCP flags are a property of the communication, and are not tied to either side of the communication.

Special Primary Rankings

FlowTraq offers a wide variety of primary rankings. Some of these are derived from multiple fields in the session record, others are derived from FlowTraq tagged fields:

- *Service Endpoint views*: Powerful view combining either server IP and server port/protocol, or client and server IP and server port/protocol. It quickly shows usage of various services in and outside of your network:

	Client and Service Endpoint				Total Bytes	Percent
1.	  10.1.1.34 10.1.1.34 AS0 (0)	→	 edge-star-shv-03-... 69.171.247.29 FACEBOOK - Facebook Inc. (32934...	: https/TCP 443/TCP	17.2 MiB	18.6% 
2.	  10.1.1.87 10.1.1.87 AS0 (0)	→	 edge-star-shv-03-... 69.171.247.29 FACEBOOK - Facebook Inc. (32934...	: https/TCP 443/TCP	9.4 MiB	10.1% 
3.	  10.1.1.87 10.1.1.87 AS0 (0)	→	 xx-fbcdn-ecmp-01-... 31.13.65.7 FACEBOOK - Facebook Inc. (32934...	: https/TCP 443/TCP	7.4 MiB	8.0% 
4.	  10.1.1.34 10.1.1.34 AS0 (0)	→	 xx-fbcdn-ecmp-01-... 31.13.65.7 FACEBOOK - Facebook Inc. (32934...	: https/TCP 443/TCP	5.6 MiB	6.0% 
5.	  10.1.1.87 10.1.1.87 AS0 (0)	→	 xx-fbcdn-ecmp-02-... 31.13.65.23 FACEBOOK - Facebook Inc. (32934...	: https/TCP 443/TCP	5.1 MiB	5.5% 

- *Autonomous System views*: FlowTraq automatically tags each IP address with the appropriate autonomous system that it belongs to. The ASN views give a high-level macro view of traffic flowing through your network, and common service destinations. Registered names for AS numbers are included and presented in the FlowTraq interface:

	Netblock	
1.	  145.244.0.0/16 145.244.0.0/16 ACONET AConet Backbone (1853)	
2.	  180.76.5.0/24 180.76.5.0/24 CNNIC-BAIDU-AP Beijing Baidu Ne...	
3.	  99.248.192.0/18 99.248.192.0/18 ROGERS-CABLE - Rogers Cable Com...	
4.	  200.88.0.0/16 200.88.0.0/16 Compañía Dominicana de Teléfono...	
5.	  37.59.0.0/16 37.59.0.0/16 OVH OVH Systems (16276)	
6.	  195.84.40.0/21 195.84.40.0/21 TDC TDC Data Networks (3292)	
7.	  67.205.64.0/18 67.205.64.0/18 IWEB-AS - iWeb Technologies Inc...	

- *NetBlock views*: Similar to AS tagging, each IP address is also tagged with the size of the network CIDR block it resides in. Often this information is available from the exporter. If not, FlowTraq will use the size of the advertised AS block that the IP address is part of. NetBlock views offer another good macro view of traffic patterns.

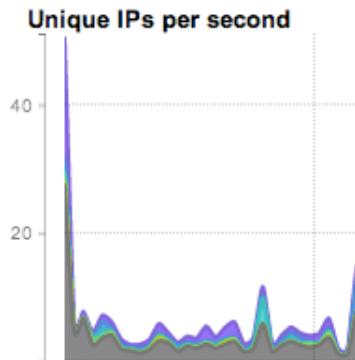
Unique Count Views

In addition to regular quantity counts, FlowTraq is also capable of ranking by the unique occurrences of other entities. These views only consider the number of uniquely different entities were observed, session and packet counts are therefore irrelevant. Examples:

- *IP addresses ranked by unique IP peers*: ranks each IP address based on the number of unique other IP addresses it communicated with.
- *Ports by unique TCP flags*: ranks each server port by the number of different TCP flag combines observed.

- *IP address by unique server port*: ranks each IP address by the number of different server ports it has contacted.

Many different combinations are possible. Unique count views can quickly find scanning and reconnaissance behavior (IP by unique port), and worm spreading and SPAM behavior (IP by unique IP). Note that graphs will usually show an initial spike as the count is performed on *first occurrence*. This is normal and expected:

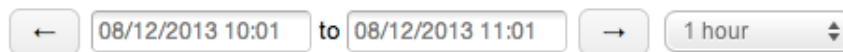


Time Navigation

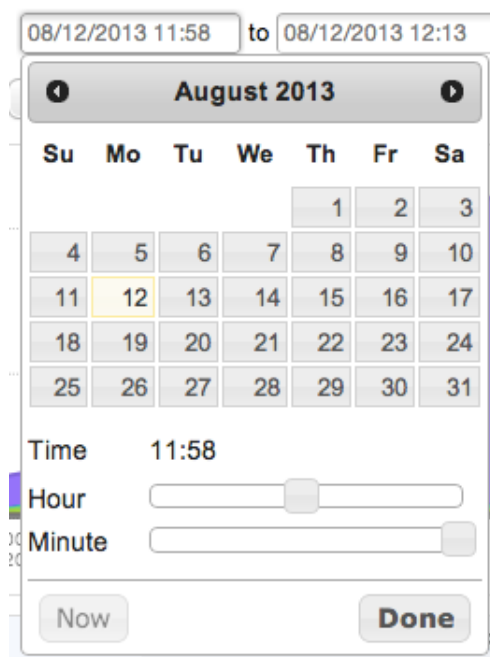
FlowTraq offers arbitrary time navigation because data is never aggregated. A history of the most recently received records is kept in RAM for quick query processing. Historical queries are serviced from the disk database, and may take longer to complete.

Absolute and Relative Time

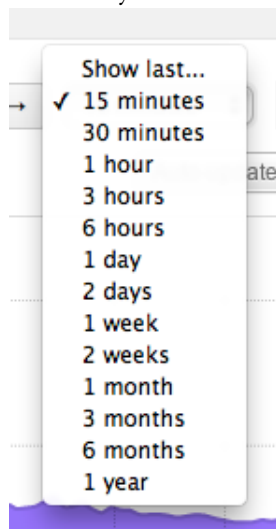
The time navigation bar in the workspace allows for absolute time selection by selecting exact dates and times, as well as relative time selection where the analyst can choose to quickly view the last N minutes or hours. Click on either of the date/time fields to display a calendar widget to select a specific time and date for selecting the timeframe of your query:



Select a date and time using the calendar and the sliders, and click *Done* when finished:



Relative time selection offers the analyst the option to quickly select a timeframe in the recent past up to now. By default the workspace displays a 15 minute view of your network:



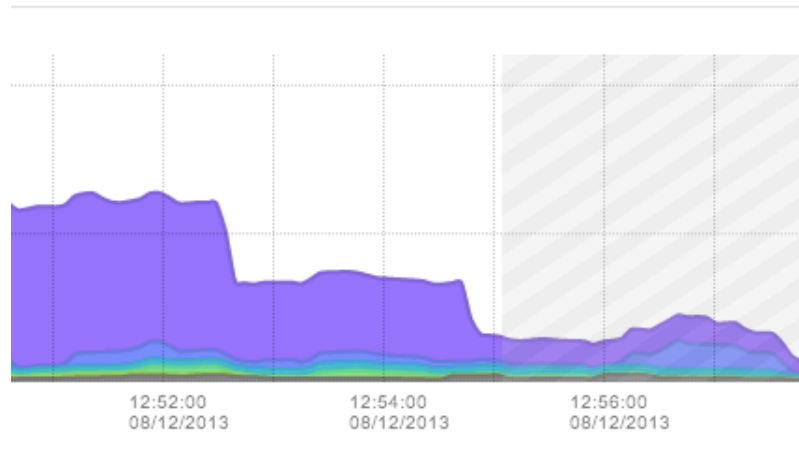
After selecting the desired timeframe through absolute or relative time the view can be refreshed by selecting the *Apply* button at the top right of the workspace.

Time Navigation

The time navigation bar displays the timestamps enclosing the currently displayed data. On either side of these timestamps are buttons to quickly move to the previous, or next timesegment of the same length as currently displayed. These *Forward/Backward* buttons allow the analyst to quickly navigate through the data by viewing the previous or next timeslice with the same view and filter.

When navigating to a timeframe that includes the current time, or any future time, a crosshatch area will be drawn on the graph indicating the traffic records are yet to be received. The crosshatch area

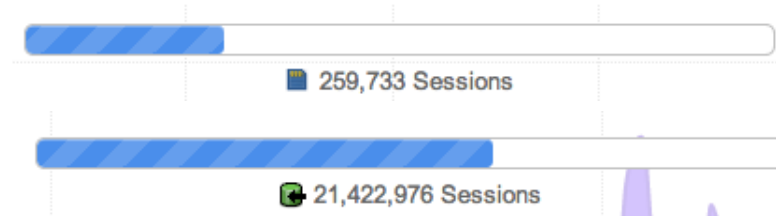
starts at approximately T-2 minutes, indicating that exporters may not yet have reported all traffic records for the most recent timeframe:



RAM vs Disk based queries

FlowTraq keeps a cache of the most recently received traffic records in RAM memory to facilitate rapid processing of queries in the most recent timeframes where analysts are most likely to be doing interactive work. For timeframes further back in history FlowTraq will query the disk database, which may take substantially longer than a RAM based query. The period for which RAM based queries can be performed is strongly dependent on the inflow rate of flow updates, and the amount of RAM dedicated to the FlowTraq system.

During query processing the icon below the process bar will indicate if the query is being serviced from RAM or from disk:



To analyze how much data is currently held in RAM and how resources are being used please refer to the administration page. The *Performance* widget displays the current RAM *Cache* fill (1% below) and the period for which queries can be serviced from RAM (3 days below):

Performance:

Connection Tracker:	444K		97%	3d
Cache:	6.9M		1%	3d
Database:	1.3B		10%	209d
Storage Performance: 10 records @ 103ms				

Workspace Operations

The table in the workspace view will display the first 10 top items. Additional pages with further ranking are available by simply navigating to the next page with the buttons at the bottom right of

each table. As the analyst moves through the various pages the graph will change to indicate which data the table is displaying. The workspace displays a top-N style ranking, so each additional data page will have a subsequently smaller contribution to the overall total.

The workspace offers a number of different interactive operations to the analyst, including tagging ranked items with userfriendly names, adding ranked items to the filter to quickly pivot the view, and a drag-to-zoom capability to further drill down on a timeframe.

Friendly Names

For operator convenience FlowTraq enables the analyst to tag certain items in the ranked view table with userfriendly names. Click on the item and select '*Set Friendly Name*' to set or change the display name of the item. Administrative users have the additional option to set the name for all the users. When this option is selected all users will see the name that the administrative user has assigned *unless* the user themselves have assigned their own friendly name to the same item. Primary ranked objects that may be tagged with a userfriendly name:

- IP address (including the addresses in IP-pair and Service Endpoint views)
- NetBlocks
- Traffic Groups
- Autonomous Systems (overrides their resolved name)
- Server Port/Protocol combinations (including those in the Service Endpoint views)
- QoS values
- VLANs
- Exporter/Interface combinations

By default IP addresses and autonomous system names are reverse-resolved *unless* a friendly name was assigned. IP addresses are reverse resolved through DNS, while AS numbers are reverse resolved in the FlowTraq server.



Select '*Set Friendly Name*' to set or change the display name of the item:



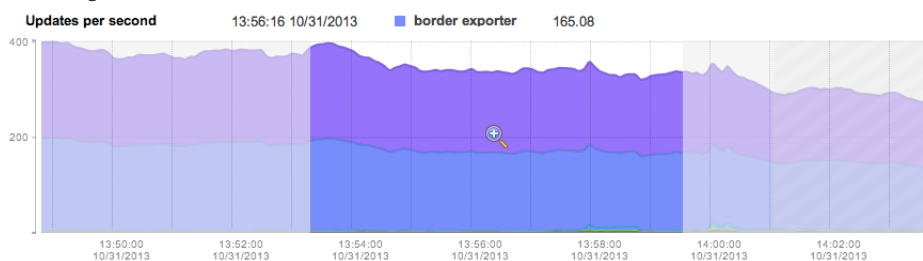
Click-to-Filter

Using the same item menu it is possible to add objects to your current filter, and either focus on their traffic, or ignore it. Keep in mind that a *'match-all'* filter combination should be used when working with an existing filter. In pairwise rankings it is possible add either side of the pairing to the filter.

Some items may offer additional filters. IP address items, for instance, will also offer the ability to filter on the autonomous system that the IP address resides in. Adding an exporter to a filter will create two filter boxes: one for the exporter IP, and one for the export protocol version.

Drag-to-Zoom

When displaying a graph the analyst may select an area of data to zoom in on by dragging the cursor over a section of the graph. When the desired zoom area is selected, a magnifying glass icon will appear. Clicking the icon will re-run the current view and filter on the selected timeframe:



Chapter 5. FlowTraq Web Interface and FlowTraq NBI Server

FlowTraq includes a web-based user interface (FlowTraq Web), which allows you to create interactive reports via a web browser, as well as the FlowTraq Network Behavioral Intelligence (NBI) Server, which allows you to configure FlowTraq's powerful NBI tools via a web interface.

This chapter details their installation.

Installation of these components is optional. You may skip directly to Chapter 3, *Initial Configuration* if you do not wish to install these components.

Software Prerequisites

We recommend installing FlowTraq Web and FlowTraq NBI Server on a Linux/Apache/PHP stack; however, many other platforms will work.



Note

Note: While FlowTraq Web Portal can connect to remote instances of FlowTraq Server, the FlowTraq Command Line Tools (which are included with FlowTraq Server) must be installed locally for FlowTraq Web Portal to function.

FlowTraq NBI Server requires a PostgreSQL Server, installed either locally or remotely. In addition, the following standard packages must be installed locally on the host:

- PHP5 interpreter and command line tools with support for Process Control (pcntl), POSIX, and PostgreSQL (pgsql)
- Web server (e.g. apache2) with PHP5 support (e.g. mod_php)



Important

We strongly recommend configuring your web server to either only accept secure https connections or to automatically redirect http requests to https.



Upcoming Changes

Future versions of FlowTraq Web Portal may have additional dependencies.

Installation Overview

In general, installing FlowTraq Web and NBI tools is a 6-step process.

1. Install FlowTraq Server.
2. Install FlowTraq Web prerequisites (apache, php, etc.)
3. Install FlowTraq Web.
4. Install FlowTraq NBI prerequisites. (postgres, php-pg, etc)
5. Configure PostgreSQL server.

6. Install FlowTraq NBI.

We have provided detailed installation guides for several common platforms. We strongly recommend using one of these platforms:

OpenSuSE Linux 11 - Installation Guide

Ubuntu Linux 10 (Lucid Lynx) - Installation Guide

CentOS 6.3 - Installation Guide

Detailed Installation Guides

OpenSuSE Linux 11 - Installation Guide

FlowTraq Server

1. Download and install FlowTraq Server by downloading the installer package, gunzipping it, and running it as root:

```
# wget http://www.flowtraq.com/downloads/flowtraq/flowtraq_Q1_13/FlowTraq-Q1_13-  
# gunzip FlowTraq-Q1_13-server-unix.sh.gz  
# sh ./FlowTraq-Q1_13-server-unix.sh.gz
```

It will unpack the binaries and startup scripts relevant for your OS, and install (by default) in /opt/flowtraq. Command-line tools can be found in /opt/flowtraq/clitools, and the NBAD/NBI toolkit is in /opt/flowtraq/nbitools.

For more information on installing FlowTraq Server, please see the FlowTraq User Manual [<http://support.flowtraq.com/Documentation>].

2. Install a license key for FlowTraq Server. The quickest way is by appending it directly to the FlowTraq configuration file. Replace the placeholders below with your own license details:

```
# echo -ne "user YOURUSERNAME\nlicense FlowTraq_FULL-XXXX-XXXX-XXXX-XXXX-XXXX-XX  
# killall -HUP flowtraq
```

Note that you can also install the license key through the desktop GUI.

FlowTraq Web

1. Using YaST, install the required software prerequisites:

```
apache2  
apache2-mod_php5  
cphp5
```

2. Download the web GUI and unpack in your webroot:

```
# cd /srv/www/htdocs
# wget http://www.flowtraq.com/downloads/flowtraq/flowtraq_Q1_13/FlowTraq-Q1_13-
# gunzip -c FlowTraq-Q1_13-web.tar.gz | tar xvf -
```



Note

This will create a directory called **flowtraq**. You will be able to access the FlowTraq web user interface by browsing to the **/flowtraq** directory on your webserver. We recommend installing in **/srv/www/htdocs/flowtraq**. If you install elsewhere, be sure to configure the **baseURL** configuration option in **config.php**.

3. Configure and launch apache. Apache needs the 'MultiViews' option to be enabled. Edit the **/etc/apache2/default-server.conf** and change the line that reads:

Options None

To:

Options Indexes MultiViews

for the default **<Directory "/srv/www/htdocs">** section.

4. In YaST->System->Services, 'ENABLE' apache2, which will start the apache webserver.

Now point your browser at **http://127.0.0.1/flowtraq** to verify that your installation was successful. Log in with username **admin** and password **admin** by default. If the Dashboard appears, but the graphs and tables do not load, then your license key may have expired. Contact FlowTraq to obtain a new license key.

You will notice that the 'Threats' page remains empty. In order to use the NBI tools from the GUI you must now install the FlowTraq NBI server.

FlowTraq NBI Server

1. Using YaST, install the following additional prerequisites:

```
php5-pcntl
php5-posix
php5-pgsql
postgresql
postgresql-server
```

2. In YaST->System->Services, 'ENABLE' postgresql, which will launch the database process. Also, restart the apache2 service, which will enable the newly installed php plugins.
3. The PostgreSQL database must be configured to work with FlowTraq. The installer of the NBI server will ask for details on the database configuration. This configuration should be created in advance:

```
# su - postgres
# psql
psql> CREATE USER flowtraq WITH PASSWORD 'pleaseuseastrongpassword';
psql> CREATE DATABASE flowtraq;
psql> GRANT ALL PRIVILEGES ON DATABASE flowtraq TO flowtraq;
psql> \q
# createlang -d flowtraq plpgsql
```

4. Next, enable password login for PostgreSQL connections. This is done by modifying the `pg_hba.conf` file. On SuSE this file is located at: `/var/lib/pgsql/data/pg_hba.conf`. Change the line that says:

```
host all all 127.0.0.1/32 ident
```

To:

```
host all all 127.0.0.1/32 md5
```

Now restart the PostgreSQL server, either through Yast->System->Services or by invoking:

```
# service postgresql restart
```

5. Download and run the FlowTraq NBI installer package:

```
# wget http://demo.flowtraq.com/downloads/flowtraq/flowtraq_Q1_13/FlowTraq-Q1_13
# gunzip FlowTraq-Q1_13-nbi_unix.sh.gz
# sh ./FlowTraq-Q1_13-nbi_unix.sh
```

The NBI installer will check to ensure that the proper prerequisites have been installed (PHP, PostgreSQL, etc).

After this, it will ask a series of questions, including the install location of the PostgreSQL database (default: 127.0.0.1), the username (default: flowtraq), and the database name (default: flowtraq). You will have to give the password for this user also.

Finally, the NBI installer will ask you for your FlowTraq server install location, which, by default is 127.0.0.1, port 9640. You will be asked to enter administrator credentials, such that the NBI installer can create a special flowtraq user that will invoke the detectors. Use a strong password for this special user.

6. You will need to provide the PostgreSQL connection information to FlowTraq Web. Open 'config-sample.php' in the `/srv/www/htdocs/flowtraq` directory for editing, and find the `NBISERVER` variable. Modify the placeholders in this variable to provide the username (flowtraq) and password (which you provided above) to the PostgreSQL database. Finally, save the modified configuration as `/srv/www/htdocs/flowtraq/config.php`

7. Return to <http://127.0.0.1/flowtraq> and visit the 'Threats' page to verify that you can now create detectors.

This concludes the installation of FlowTraq Web and FlowTraq NBI Server.

Ubuntu Linux 10 (Lucid Lynx) - Installation Guide

FlowTraq Server

1. Download and install FlowTraq Server by downloading the installer package, gunzipping it, and running it as root:

```
# wget http://www.flowtraq.com/downloads/flowtraq/flowtraq_Q1_13/FlowTraq-Q1_13-  
# gunzip FlowTraq-Q1_13-server-unix.sh.gz  
# sh ./FlowTraq-Q1_13-server-unix.sh.gz
```

It will unpack the binaries and startup scripts relevant for your OS, and install (by default) in /opt/flowtraq. Command-line tools can be found in /opt/flowtraq/clitools, and the NBAD/NBI toolkit is in /opt/flowtraq/nbitools.

For more information on installing FlowTraq Server, please see the FlowTraq User Manual [<http://support.flowtraq.com/Documentation>].

2. Install a license key for FlowTraq Server. The quickest way is by appending it directly to the FlowTraq configuration file. Replace the placeholders below with your own license details:

```
# echo -ne "user YOURUSERNAME\nlicense FlowTraq_FULL-XXXX-XXXX-XXXX-XXXX-XXXX-XX  
# killall -HUP flowtraq
```

Note that you can also install the license key through the desktop GUI.

3. Modify your firewall settings to allow incoming NetFlow, sFlow, etc:

```
# ufw allow 2055
```

FlowTraq Web

1. Install the required software prerequisites:

```
# apt-get install apache2 php5 libapache2-mod-php5 php5-cli
```

2. Download the web GUI and unpack in your webroot:

```
# cd /var/www  
# wget http://www.flowtraq.com/downloads/flowtraq/flowtraq_Q1_13/FlowTraq-Q1_13-  
# gunzip -c FlowTraq-Q1_13-web.tar.gz | tar xvf -
```



Note

This will create a directory called **flowtraq**. You will be able to access the FlowTraq web user interface by browsing to the **/flowtraq** directory on your webserver. We recommend installing in **/var/www**. If you install elsewhere, be sure to configure the **baseURL** configuration option in **config.php**.

3. Configure and launch apache. Apache needs the 'MultiViews' option to be enabled. Edit the **/etc/apache2/sites-available/default** file and, if needed change the block that reads:

```
Options ...  
</Directory>
```

To:

```
Options ... MultiViews  
</Directory>
```

in the **<Directory "/var/www">** section.

4. Restart apache2, which will start the apache webserver and enable your changes:

```
# /etc/init.d/apache2 restart
```

Now point your browser at **http://127.0.0.1/flowtraq** to verify that your installation was successful. Log in with username **admin** and password **admin** by default. If the Dashboard appears, but the graphs and tables do not load, then your license key may have expired. Contact FlowTraq to obtain a new license key.

You will notice that the 'Threats' page remains empty. In order to use the NBI tools from the GUI you must now install the FlowTraq NBI server.

FlowTraq NBI Server

1. Install the following additional prerequisites:

```
# apt-get install postgresql php5-pgsql postgresql-client
```

2. Relaunch apache2, which will start the apache webserver and enable your changes:

```
# /etc/init.d/apache2 restart
```

3. The PostgreSQL database must be configured to work with FlowTraq. The installer of the NBI server will ask for details on the database configuration. This configuration should be created in advance:

```
# su - postgres
# psql
psql> CREATE USER flowtraq WITH PASSWORD 'pleaseuseastrongpassword';
psql> CREATE DATABASE flowtraq;
psql> GRANT ALL PRIVILEGES ON DATABASE flowtraq TO flowtraq;
psql> \q
# createlang -d flowtraq plpgsql
```

4. Next, enable password login for PostgreSQL connections. This is done by modifying the `pg_hba.conf` file. On Ubuntu this file is located at: `/etc/postgresql/<version number>/main/pg_hba.conf`. Edit the file and, if needed, change the line that says:

```
host all all 127.0.0.1/32 ident
```

To:

```
host all all 127.0.0.1/32 md5
```

Now restart the PostgreSQL server:

```
# /etc/init.d/postgresql restart
```

5. Download and run the FlowTraq NBI installer package:

```
# wget http://demo.flowtraq.com/downloads/flowtraq/flowtraq_Q1_13/FlowTraq-Q1_13
# gunzip FlowTraq-Q1_13-nbi_unix.sh.gz
# sh ./FlowTraq-Q1_13-nbi_unix.sh
```

The NBI installer will check to ensure that the proper prerequisites have been installed (PHP, PostgreSQL, etc).

After this, it will ask a series of questions, including the install location of the PostgreSQL database (default: 127.0.0.1), the username (default: flowtraq), and the database name (default: flowtraq). You will have to give the password for this user also.

Finally, the NBI installer will ask you for your FlowTraq server install location, which, by default is 127.0.0.1, port 9640. You will be asked to enter administrator credentials, such that the NBI installer can create a special flowtraq user that will invoke the detectors. Use a strong password for this special user.

6. You will need to provide the PostgreSQL connection information to FlowTraq Web. Open 'config-sample.php' in the `/var/www/flowtraq` directory for editing, and find the `NBISERVER` variable. Modify the placeholders in this variable to provide the username (flowtraq) and password (which you provided above) to the PostgreSQL database. Finally, save the modified configuration as `/var/www/flowtraq/config.php`

7. Return to <http://127.0.0.1/flowtraq> and visit the 'Threats' page to verify that you can now create detectors.

This concludes the installation of FlowTraq Web and FlowTraq NBI Server.

CentOS 6.3 - Installation Guide

FlowTraq Server

1. Download and install FlowTraq Server by downloading the installer package, gunzipping it, and running it as root:

```
# yum install wget
# wget http://www.flowtraq.com/downloads/flowtraq/flowtraq_Q1_13/FlowTraq-Q1_13-
# gunzip FlowTraq-Q1_13-server-unix.sh.gz
# sh ./FlowTraq-Q1_13-server-unix.sh.gz
```

It will unpack the binaries and startup scripts relevant for your OS, and install (by default) in /opt/flowtraq. Command-line tools can be found in /opt/flowtraq/clitools, and the NBAD/NBI toolkit is in /opt/flowtraq/nbitools.

For more information on installing FlowTraq Server, please see the FlowTraq User Manual [<http://support.flowtraq.com/Documentation>].

2. Install a license key for FlowTraq Server. The quickest way is by appending it directly to the FlowTraq configuration file. Replace the placeholders below with your own license details:

```
# echo -ne "user YOURUSERNAME\nlicense FlowTraq_FULL-XXXX-XXXX-XXXX-XXXX-XXXX-XX
# /etc/init.d/flowtraq restart
```

Note that you can also install the license key through the desktop GUI.

FlowTraq Web

1. Install the required software prerequisites:

```
# yum install httpdmod_ssl php php-process
```

2. Download the web GUI and unpack in your webroot:

```
# cd /var/www/html/html
# wget http://www.flowtraq.com/downloads/flowtraq/flowtraq_Q1_13/FlowTraq-Q1_13-
# gunzip -c FlowTraq-Q1_13-web.tar.gz | tar xvf -
```



Note

This will create a directory called `flowtraq`. You will be able to access the FlowTraq web user interface by browsing to the `/flowtraq` directory on your webserver. We rec-

commend installing in `/var/www/html`. If you install elsewhere, be sure to configure the `baseURL` configuration option in `config.php`.

3. Configure and launch apache. Apache needs the 'MultiViews' option to be enabled. Edit the `/etc/httpd/conf/httpd.conf` file and, if needed change the line that reads:

```
Options Indexes FollowSymLinks
```

To:

```
Options Indexes FollowSymLinks MultiViews
```

in the `<Directory "/var/www/html">` section.

4. Start the apache webserver, and set it to start by default:

```
# service httpd start
# /sbin/chkconfig httpd on
```

5. Turn off SELinux. CentOS 5 turns on SELinux by default, which prevents Apache from running outside tools via CGI, including the FlowTraq command line tools. Because `/opt/flowtraq` is outside the `httpd_t` domain, `httpd` cannot access it. More information can be found at <http://wiki.centos.org/HowTos/SELinux>

The simplest way to deal with this is to put SELinux into permissive mode. To do so, edit `/etc/selinux/config` and change

```
SELINUX=enforcing
```

To:

```
SELINUX=permissive
```

Then run:

```
# setenforce permissive
```

If you cannot put SELinux into permissive mode, please see the following knowledge base for a workaround which involves making FlowTraq part of the `httpd` security domain: Knowledge Base Article [<http://support.flowtraq.com/viewtopic.php?f=4&t=99>].

6. Now point your browser at `http://127.0.0.1/flowtraq` to verify that your installation was successful. Log in with username `admin` and password `admin` by default. If the Dashboard appears, but the graphs and tables do not load, then your license key may have expired. Contact FlowTraq to obtain a new license key.

You will notice that the 'Threats' page remains empty. In order to use the NBI tools from the GUI you must now install the FlowTraq NBI server.

FlowTraq NBI Server

1. Install the following additional prerequisites:

```
# yum install postgresql postgresql-server php-pgsql
```

2. Initialize and start postgresql:

```
# service postgresql initdb
# service postgresql start
```

Set postgres to be started on reboot:

```
# /sbin/chkconfig postgresql on
```

Also, restart the apache2 service, to enable the newly installed php plugins.

```
# service httpd start
```

3. The PostgreSQL database must be configured to work with FlowTraq. The installer of the NBI server will ask for details on the database configuration. This configuration should be created in advance:

```
# su - postgres
# psql
psql> CREATE USER flowtraq WITH PASSWORD 'pleaseuseastrongpassword';
psql> CREATE DATABASE flowtraq;
psql> GRANT ALL PRIVILEGES ON DATABASE flowtraq TO flowtraq;
psql> \q
# createlang -d flowtraq plpgsql
```

4. Next, enable password login for PostgreSQL connections. This is done by modifying the `pg_hba.conf` file. On CentOS this file is located at: `/var/lib/pgsql/data/pg_hba.conf`. Edit the file and, if needed, change the line that says:

```
host all all 127.0.0.1/32 ident
```

To:

```
host all all 127.0.0.1/32 md5
```

Now restart the PostgreSQL server:

```
# service postgresql restart
```

5. Download and run the FlowTraq NBI installer package:

```
# wget http://demo.flowtraq.com/downloads/flowtraq/flowtraq_Q1_13/FlowTraq-Q1_13
# gunzip FlowTraq-Q1_13-nbi_unix.sh.gz
# sh ./FlowTraq-Q1_13-nbi_unix.sh
```

The NBI installer will check to ensure that the proper prerequisites have been installed (PHP, PostgreSQL, etc).

After this, it will ask a series of questions, including the install location of the PostgreSQL database (default: 127.0.0.1), the username (default: flowtraq), and the database name (default: flowtraq). You will have to give the password for this user also.

Finally, the NBI installer will ask you for your FlowTraq server install location, which, by default is 127.0.0.1, port 9640. You will be asked to enter administrator credentials, such that the NBI installer can create a special flowtraq user that will invoke the detectors. Use a strong password for this special user.

6. You will need to provide the PostgreSQL connection information to FlowTraq Web. Open 'config-sample.php' in the `/var/www/html/flowtraq` directory for editing, and find the NBISERVER variable. Modify the placeholders in this variable to provide the username (flowtraq) and password (which you provided above) to the PostgreSQL database. Finally, save the modified configuration as `/var/www/html/flowtraq/config.php`
7. Return to `http://127.0.0.1/flowtraq` and visit the 'Threats' page to verify that you can now create detectors.

This concludes the installation of FlowTraq Web and FlowTraq NBI Server.

Access

After installation, you may access FlowTraq Web by pointing a web browser to `http://127.0.0.1/flowtraq` (or similar, depending on the address / hostname and location you installed FlowTraq Web).



Note

The default username and password for the initial user is admin/admin.

Installation Troubleshooting

Error: NBI server not configured.

The variable NBISERVER was not defined in config.php, or config.php was not found.

NBISERVER specifies the database connection string used to connect to the NBI PostgreSQL database. Edit `/path/to/webroot/config.php` (if this file does not exist, please create it using `/path/to/webroot/config-sample.php` as a template). Set NBISERVER to a valid PostgreSQL connection string corresponding to the PostgreSQL database you previously set up for FlowTraq NBI. For more information on PostgreSQL connection strings, see `pg_connect()` [<http://php.net/manual/en/function.pg-connect.php>].

Error: NBI server authentication failed.

The connection string specified in `config.php`'s NBISERVER was not defined in `config.php`.

Ensure that PostgreSQL is installed, that password identification is enabled (`pg_hba.conf`). Then make sure the host, database, username, and password specified in the NBISERVER variable in `config.php` are valid. For more information, please see Chapter 5, *FlowTraq Web Interface and FlowTraq NBI Server*.

Error: The FlowTraq Server failed to identify itself.

The version of FlowTraq Server is too old to support the identification and authentication methods required by FlowTraq NBI Server. Please upgrade FlowTraq Server to version Q1/13 or greater.

Warning: The NBI server is not authenticated with this FlowTraq server.

To reauthenticate the NBI Server to FlowTraq Server, uninstall FlowTraq NBI and reinstall. During installation, be sure to provide the the installer with the credentials of a valid admin user.

```
# /opt/flowtraq-nbi/uninstall.sh
# rm -rf /opt/flowtraq-nbi
# wget http://demo.flowtraq.com/downloads/flowtraq/flowtraq_Q1_13/FlowTraq-Q1_13-n
# gunzip FlowTraq-Q1_13-nbi_unix.sh.gz
# sh ./FlowTraq-Q1_13-nbi_unix.sh
```

Chapter 6. Configuring Flow Sources

After installing FlowTraq and performing the initial configuration, it is time to configure your network devices to begin exporting flow data to FlowTraq.

Supported Input Formats

FlowTraq is designed to support the vast majority of flow formats. Instead of listing all compatible devices, we list supported formats. Please refer to your equipment manufacturer's documentation for details on your specific device.

NetFlow v1, v5, v7, and v9

The NetFlow format was designed by CISCO, and one or more versions of NetFlow are supported by the vast majority of their devices. NetFlow is a *push protocol* and FlowTraq listens on the default port, so only your sending devices need to be configured in order to use NetFlow. NetFlow datagrams are generally sent to port UDP/2055.



NetFlow and IPv6

Use NetFlow v9 if you have IPv6 traffic on your network, as it is the only version to support IPv6.

cFlow and jFlow

These formats are variations on the NetFlow v5. Ports UDP/9666 and UDP/9996 are sometimes used instead of or in addition to UDP/2055. FlowTraq Server supports listening on multiple ports, so deployments in mixed environments are not a problem.

IPFIX (both TCP and UDP)

Like NetFlow, IPFIX is a push protocol. By default, FlowTraq listens for IPFIX over UDP on port 2055. Configure alternative or additional listen ports in the Exporters panel in Preferences.

By default, FlowTraq is not configured to listen for IPFIX over TCP. You can configure a listen port or ports in the Exporters panel in Preferences.

sFlow v2, v4, and v5

The sFlow format is a scalable sampled flow format. In contrast to NetFlow, it is not a push protocol. Rather, it is up to the collector to configure the source via SNMP. FlowTraq Server uses SNMPv2 to configure sFlow-capable devices. Export packets are generally sent to port UDP/6343.

CISCO NSEL (ASA Firewall Events)

FlowTraq accepts Network Secure Event Logging (NSEL) from the CISCO ASA firewall line. The NSEL events (flow created, flow deleted, flow denied) are packaged in NetFlow version 9 templates, and FlowTraq allows you to search for all three event types as well as the extended event codes (typically, explanations for why a flow was denied).

Like NetFlow, NSEL events are push updates. On the collector side, NSEL is configured in the same way as NetFlow version 9.

Please note that the ASA firewall flow exports contain less information than NetFlow updates. FlowTraq uses heuristics to infer some of the missing information.

 Tip

If you don't have flow export-capable hardware, or if you prefer NetFlow to the format your hardware uses, you may use Flow Exporter, a free software-based flow sensor we develop as a companion to FlowTraq.

Please see the section called “Using Flow Exporter” for more information on Flow Exporter.

Configuring NetFlow, cFlow, jFlow, IPFIX, and NSEL

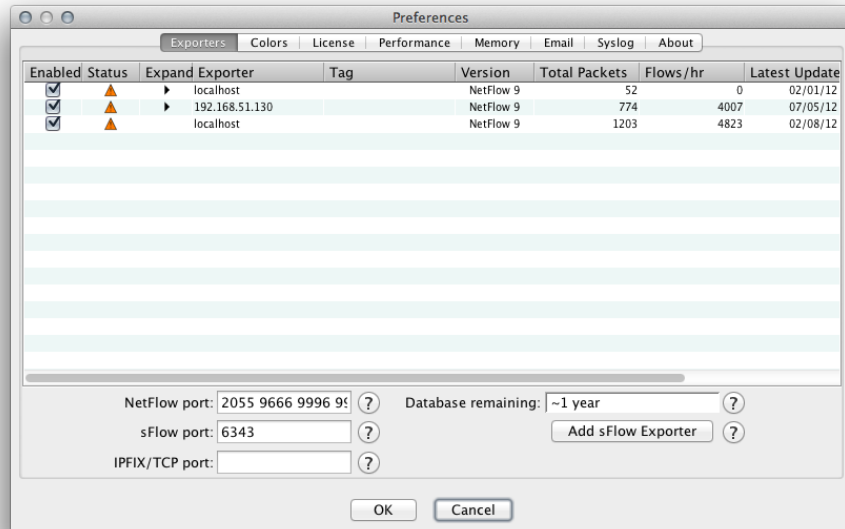
Because these protocols are push protocols, you must configure the flow source device to send flow updates to FlowTraq. See Appendix A, *Enabling Flow Export on Common Devices* for quick-start guides for enabling flow export on common devices, or consult your network device's documentation for more information.

By default, FlowTraq listens for NetFlow, cFlow, jFlow, IPFIX, and NSEL updates on UDP ports 2055, 9666, and 9996. In general, we recommend you use the default ports, but you may change them or configure additional listen ports.

 Configuring Additional NetFlow, cFlow, jFlow, IPFIX, and NSEL Listen Ports

To configure additional NetFlow listen ports, take the following steps.

1. Log in to FlowTraq as an administrative user.
2. Click the *Preferences* button on the Dashboard window's toolbar, or select *Edit > Preferences* from the menu.
3. Select the *Exporters* tab.



4. Add listen ports to the appropriate space-separated list and click "OK" to cause FlowTraq to start listening for flow updates on those ports.

For UDP push protocols (that is, NetFlow, cFlow, jFlow, IPFIX over UDP, and NSEL) enter ports in the "Netflow" list. For TCP push protocols (IPFIX over TCP), use the IPFIX/TCP line.



Tip

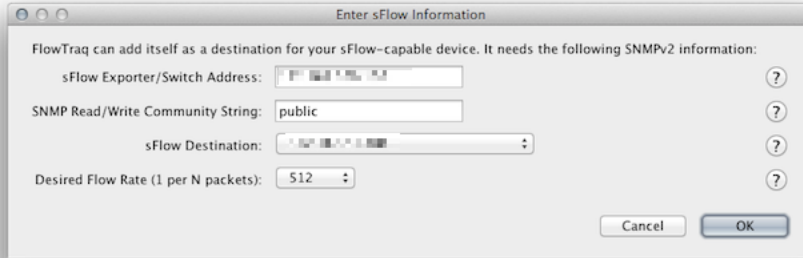
Each exporter will display either a green light or an "alert" triangle. The green light indicates that flows are being received, while the alert triangle is displayed when FlowTraq has not received any updates from the exporter in a while, or if FlowTraq is having a problem interpreting the updates from that exporter. Move your mouse cursor over the triangle to see the cause of the alert.

Configuring sFlow

FlowTraq Server is capable of automatically configuring sFlow devices though the sFlow MIB using SNMPv2. To set up an sFlow device, you must supply FlowTraq with configuration information as described below; FlowTraq will then attempt to register itself with the device. It will continue to refresh that request every 20 minutes for as long as that exporter remains active in the Exporters preference panel.

To set up an sFlow device from within FlowTraq, take the following steps.

1. Log in to FlowTraq as an Administrator.
2. Click the *Preferences* button on the Dashboard window's toolbar, or select *Edit > Preferences* from the menu.
3. Select the *Exporters* tab.
4. At the bottom of the tab select *Add sFlow Exporter*. You will see a window similar to this one:



Important

To enable an sFlow exporter, you need to supply FlowTraq with the following pieces of information:

sFlow Exporter/Switch Address	The IP address of the exporter or switch that will be sending sFlow to the FlowTraq server. IPv4 and IPv6 are both supported. This is the address to which the FlowTraq server will attempt to connect using SNMPv2 to configure the exporter. It is important that FlowTraq Server can reach this IP address on the network.
SNMP Read/Write Community String	The community string for read/write is effectively the password for configuring the exporter. The Management Information Base must be written with the flow destination in order for sFlow exporting to work.
sFlow Destination	This is the address of the machine running FlowTraq Server that the exporter will send the sFlow packets to. The list is populated with all the IPv4 and IPv6 addresses that are currently configured on FlowTraq Server. FlowTraq will try to automatically select the right IP address as an export destination; however, this automatic selection may not always be correct. If the IP address is not correct, enter or select the correct one here.
Desired Flow Rate	sFlow is a sampling technology that uses a probabilistic 1-in-N sampling rate. This means that, on average, one in every N packets gets sent to the collector (although not necessarily exactly every Nth packet). By selecting lower values for this field (such as 1-in-128 or 1-in-256), the accuracy of your collected flow information will go up; however, so will the load on your sFlow exporter, and the volume of export traffic between the exporter and FlowTraq Server. If you are monitoring a very busy connection, it might be worth selecting higher values (such as 1-in-2048). In fact, a busy exporter may decide to reduce the sampling rate on its own to reduce its CPU load.

5. Enter the information in the window and click *OK* .

After you complete these steps, the sFlow exporter is added to the exporters list, and the SNMPv2 engine will attempt to configure the exporter using the sFlow Management Information Base (MIB).

 Tip

Both enterprise 4300 (version 1.2) and 14706 (version 1.3) are supported, and FlowTraq Server will attempt to configure the sFlow-capable device through both MIBs automatically. When multiple input ports are specified for sFlow, the SNMPv2 engine will use a round-robin scheme when assigning destination ports to sFlow exporters. This effectively spreads the load of multiple incoming sFlow streams over multiple processing threads in FlowTraq Server.

Using Flow Exporter

In addition to using export capable hardware devices, it is also possible to use Flow Exporter to export NetFlow v5 or NetFlow v9 to FlowTraq Server. Listed below are some reasons to consider using Flow Exporter.

- A NetFlow-, sFlow-, jFlow-, or cFlow-capable device is not available. For instance, your hardware may not support flow export, or you may be monitoring virtual machines on which you do not have access or permissions to configure the routing or switching hardware.
- You would prefer to avoid putting the additional CPU and memory load on your switch or router and instead would like to use a network tap or the more lightweight port mirroring (or SPAN port) feature instead.
- You would like to monitor traffic at specific hosts or servers. (This is particularly useful in cloud deployments.)
- You have access to packet capture files (PCAP) and would like to convert those into flows for analysis through FlowTraq.

Flow Exporter has the same platform support as FlowTraq. Please refer to <http://www.flowtraq.com/corporate/product/flow-exporter> for more information on installation and configuration.

Troubleshooting Flow Sources

Below are the most common reasons FlowTraq why may not be displaying the flows that you expect it to. Most of the time, the reason for lack of traffic is one of the following:

A firewall is blocking inbound flow traffic

The most common cause of missing flow traffic is a firewall blocking the ports needed to receive flow updates.

The firewall may be somewhere on the network or on the FlowTraq host itself. Most systems have host-based firewalls configured to block inbound traffic on certain ports. On some versions of Windows, Windows Firewall blocks flow ports by default; RedHat Enterprise Linux and CentOS also ship with a firewall configured by default. Take a look at your firewall configuration to see if you might have this problem.

Make sure that traffic on UDP/2055 (NetFlow/IPFIX), UDP/9666 and UDP/9996 (cFlow/jFlow), UDP/6343 (sFlow),

and any other ports on which you configured flow collection can reach FlowTraq Server.

FlowTraq is unable to bind the required ports

FlowTraq Server will not be able to collect any flow data if another flow collector is running on the same system because it will be unable to bind the required listen ports.

The `netstat` tool can tell you which process id or executable has the required ports bound. On UNIX hosts (including Mac OS X),

```
# netstat -a -p
```

or, on Windows,

```
# netstat -a -o -b
```

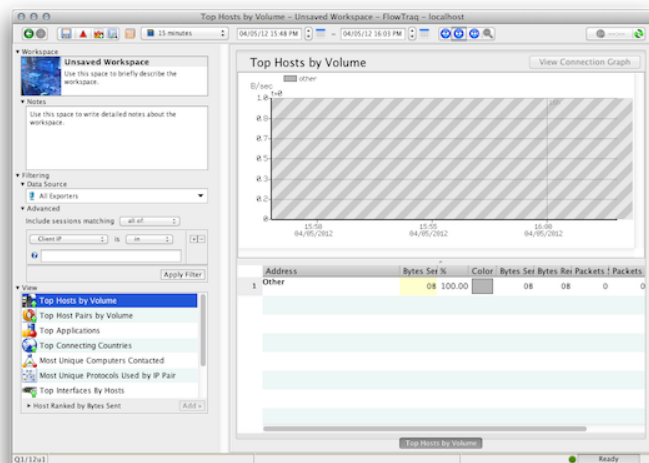
will, if run with admin permissions, show which processes have bound which ports.

If a process other than `flowtraq` has bound the required UDP ports, you will need to shut down that process or reconfigure both FlowTraq and your NetFlow exporter to use a different port.

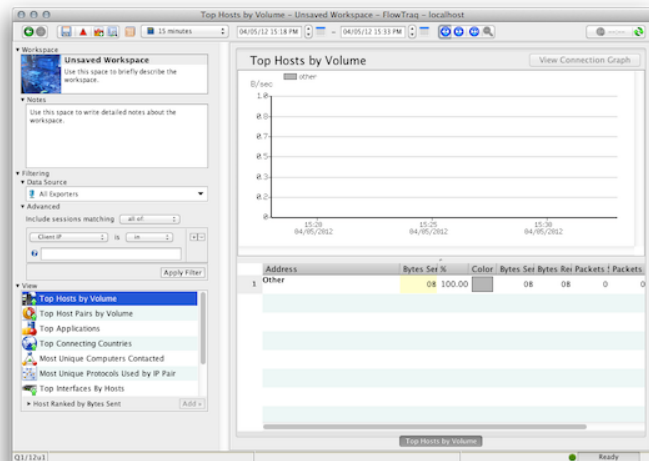
Significant system time skew between Client and Server

If FlowTraq Client is running on a machine with a significantly different system clock time than the host running FlowTraq Server, a query for a recent time frame can cause the server to try to fetch sessions that it considers to be in the future or far in the past. In either case, the result set might be empty.

If the cross-hatch area in the graph is covering the entire screen, as pictured below, the client clock is in the future compared to the server clock:

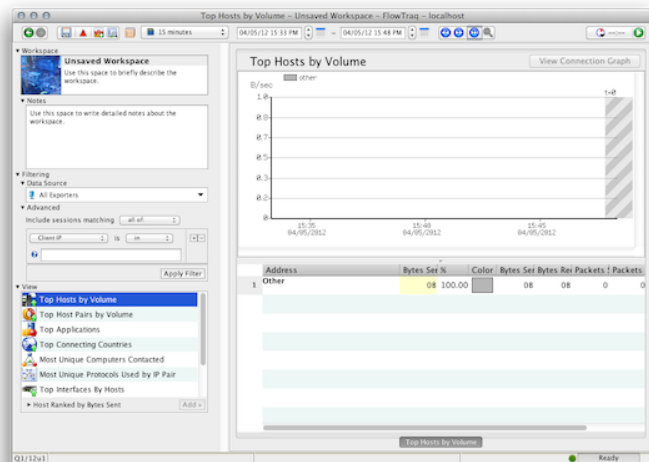


If the cross-hatch area is not showing at all, the client is in the past:



In either case, try moving or extending your time selection back or forward in time until you see a graph showing sessions.

We strongly recommend remedying time skew issues by adjusting system clocks; otherwise, alerts and reports may be also misconfigured. If clocks are aligned, the cross-hatch area should occupy a thin strip on the right only:



"Template Not Found" (NetFlow v9 and IPFIX only)

The NetFlow v9 and IPFIX formats use a template-based system where the flow export datagram format is described by a template. This format can differ from exporter to exporter, and each exporter will publish a template record approximately every 10 minutes. The collector determines how to parse the NetFlow v9 datagrams from that particular exporter based on the published template. It is possible that flow records are arriving, but no template has yet been seen; in this case, FlowTraq must ignore the records until it receives a template in order to avoid interpreting a record incorrectly. In some cases it might take up to 20 minutes before a template is received.

Check the Exporters tab in the configuration panel. If your NetFlow v9 or IPFIX exporter is shown there, it has successfully sent traffic to FlowTraq Server. However, it may still be waiting for a template record, and until that time, no sessions will appear.

Incorrectly Configured Exporter

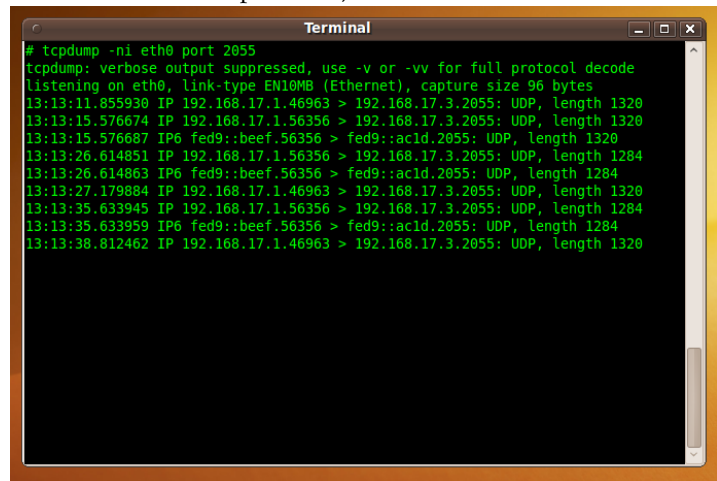
It is possible that the configuration on your exporter is incorrect. For instance, you may have mistyped the destination IP or port, or enabled flow on an unused port.

To verify that your exporter is working correctly, capture some traffic on the host running FlowTraq Server and confirm that flow traffic is arriving at the expected port.

On Unix systems (including Mac OS X), you can use the following `tcpdump` command to capture UDP/2055 traffic on the interface called `IFACE` (typically, `eth0` or `en0`):

```
# tcpdump -i IFACE port 2055
```

(You may need to use the `ifconfig` command to determine which interface to capture on.)

A terminal window titled "Terminal" with a black background and green text. It shows the command `# tcpdump -ni eth0 port 2055` and its output. The output indicates that tcpdump is listening on `eth0` and capturing traffic on port 2055. It shows several lines of captured traffic, including IP addresses, ports, and lengths. For example, it shows traffic from `192.168.17.1.46963` to `192.168.17.3.2055` and from `192.168.17.1.56356` to `192.168.17.3.2055`.

```
# tcpdump -ni eth0 port 2055
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
13:13:11.855930 IP 192.168.17.1.46963 > 192.168.17.3.2055: UDP, length 1320
13:13:15.576674 IP 192.168.17.1.56356 > 192.168.17.3.2055: UDP, length 1320
13:13:15.576687 IP6 fed9::beef.56356 > fed9::acd.2055: UDP, length 1320
13:13:26.614851 IP 192.168.17.1.56356 > 192.168.17.3.2055: UDP, length 1284
13:13:26.614863 IP6 fed9::beef.56356 > fed9::acd.2055: UDP, length 1284
13:13:27.179884 IP 192.168.17.1.46963 > 192.168.17.3.2055: UDP, length 1320
13:13:35.633945 IP 192.168.17.1.56356 > 192.168.17.3.2055: UDP, length 1284
13:13:35.633959 IP6 fed9::beef.56356 > fed9::acd.2055: UDP, length 1284
13:13:38.812462 IP 192.168.17.1.46963 > 192.168.17.3.2055: UDP, length 1320
```

On Windows systems, we recommend the open-source packet-capture software Wireshark for this purpose. Wireshark is available at <http://www.wireshark.org/>.

Chapter 7. The Dashboard

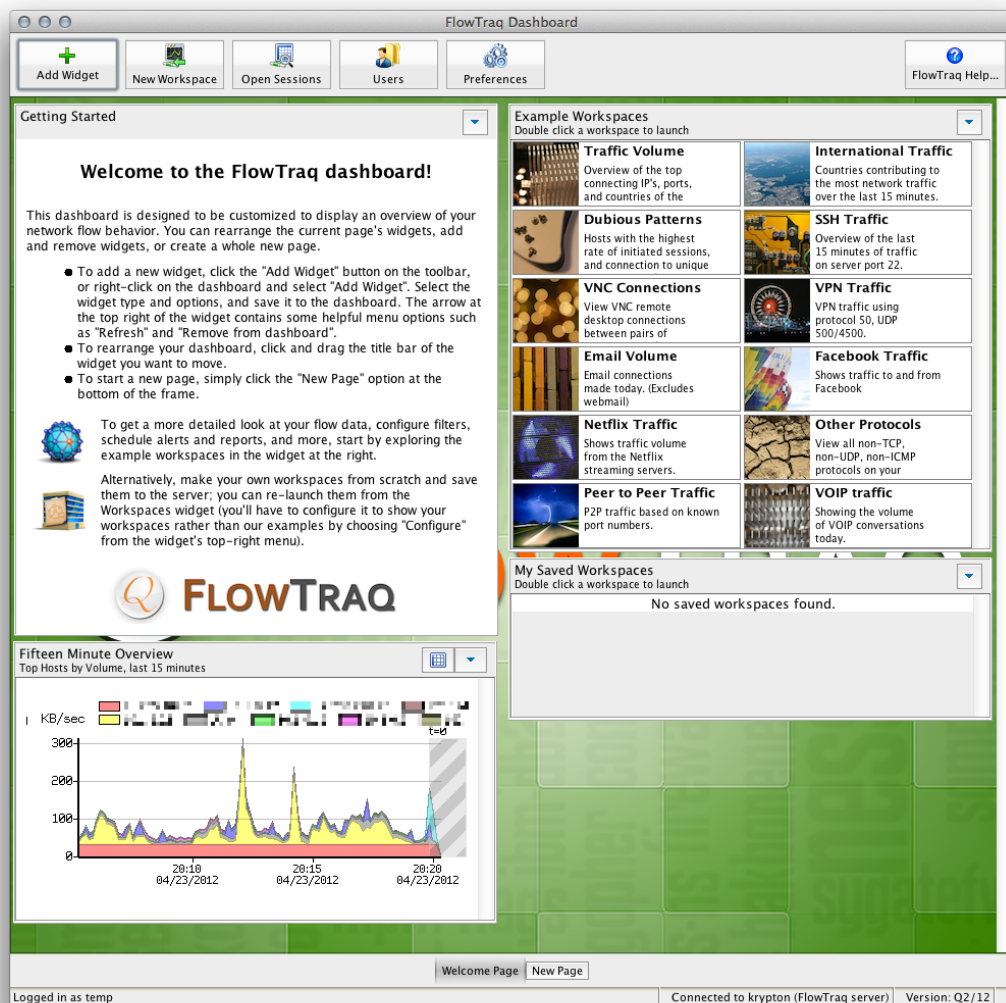
The Dashboard is the first window you see when you log in to FlowTraq. It has several functions:

- It provides a customizable, at-a-glance overview of the activity on your network.
- It is the launching point for conducting deeper investigations in Workspaces (see Chapter 8, *Interactive Reports (Workspaces)*) or the Session Explorer (see Chapter 10, *Session Explorer*), and for resuming investigations-in-progress.
- It provides access to the contents of scheduled Reports (see Chapter 9, *Scheduled Reports*) and the list of Alert notifications (see Chapter 11, *Alerts and Notifications*).
- It provides access to the user-specific preference panels.
- For administrative users, it provides access to the system-wide preference control panels, as well as the user administration control panel.

This chapter describes the Dashboard in depth.

Setting Up Your Dashboard

The first time a user logs in, that user's Dashboard is pre-set to include a few widgets, including a "Welcome" message, a Workspaces widget showing some preconfigured Workspaces, an (initially empty) Workspaces widget which provides access to Workspaces you save, and a few other informational widgets.

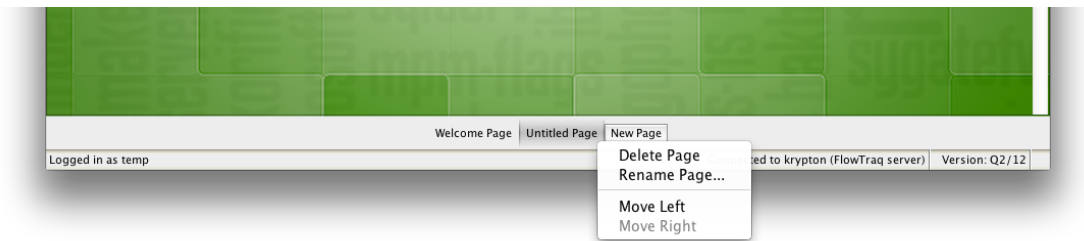


Important

Your dashboard is *your* Dashboard. Each FlowTraq user can customize their own Dashboard to their specifications.

By the same token, we do not recommend sharing user profiles or logging in from multiple locations at the same time, as user data synchronization issues can occur. There are no limitations on the number of user accounts you can configure, so please configure one user for each person in your organization who will be using FlowTraq.

Pages



Initially, the Dashboard only has one page. Pages can be added, removed, renamed, and rearranged in the following ways:

- To add a page, click the "New Page" button at the bottom of the Dashboard window.
- To remove, rename, or move an existing page, right-click on the name of the page and select the appropriate option.

Multi-column Layout

Each page can have two, three, or four columns of widgets. To change the number of columns a page has, right-click on the name of the page and select the "Two Columns", "Three Columns", or "Four Columns".

Managing Widgets

Widgets can be added, removed, rearranged, and configured in a variety of ways to give insight into the information most pertinent to your needs.

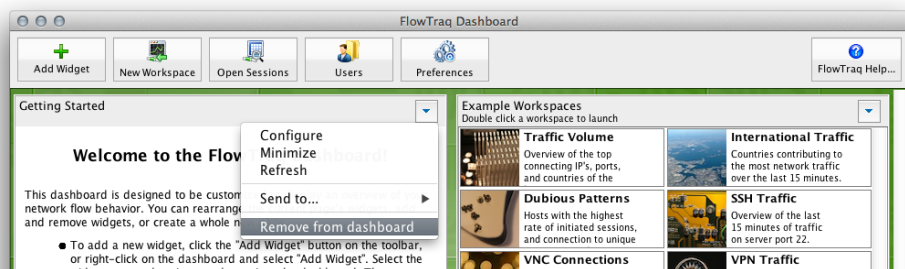
- To add a widget, click the "Add Widget" button on the Dashboard Toolbar, or right-click on some empty space in the Dashboard and select "Add Widget." An unconfigured widget will appear. Complete the widget configuration by naming the widget, selecting the widget type from the dropdown, choosing an automatic refresh interval, and completing the rest of the widget's configuration. Finally, click "Save", and the new widget will appear.



- To remove a widget, right-click on the widget menu button, which is located on the right-hand side of the widget's title bar, and select "Remove Widget."

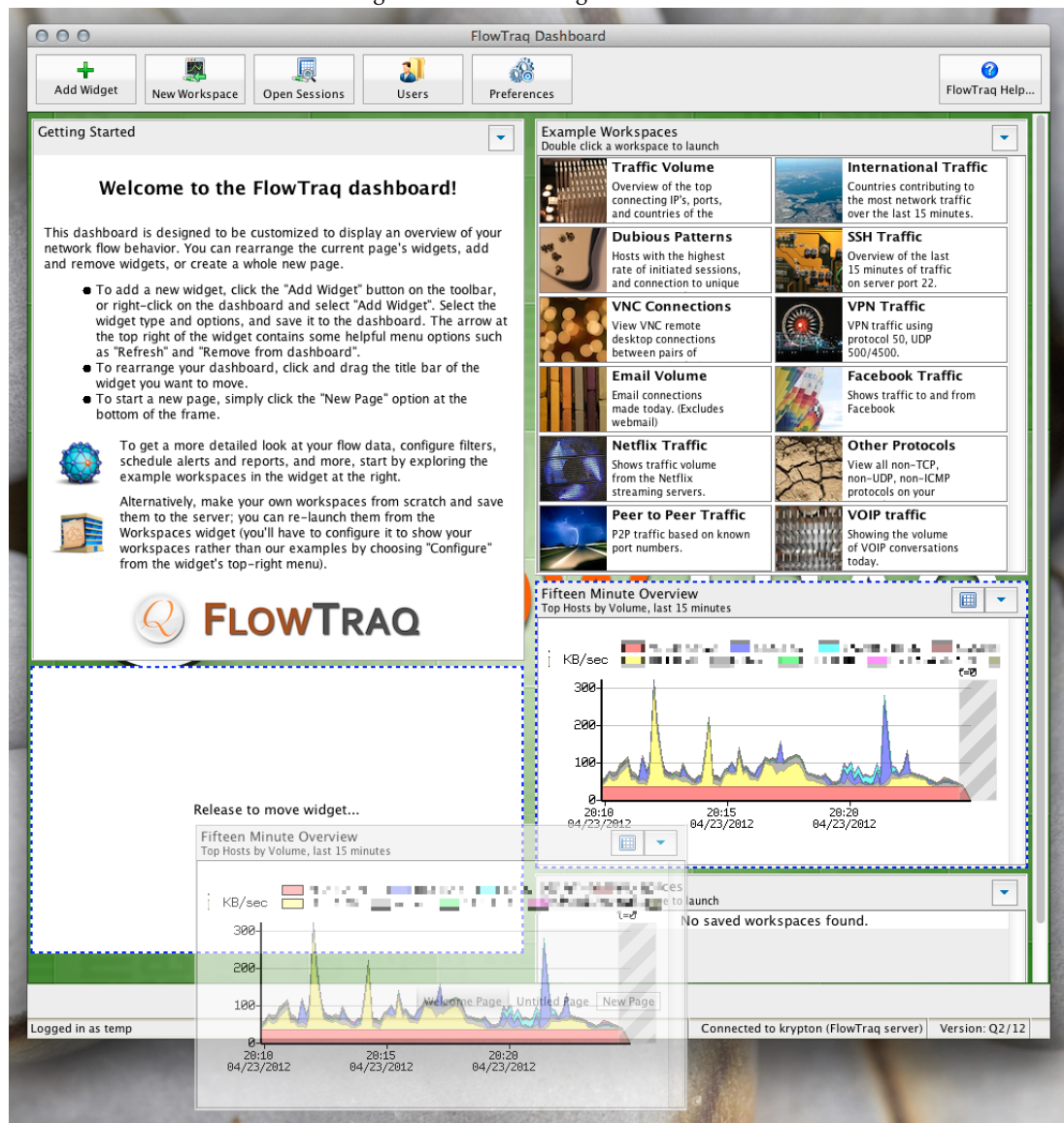


Important



You cannot undo this action.

- To move a widget to another location on the same Dashboard page, drag its title bar to where you would like to move it. A "landing-zone" will appear in the spot where the widget will be moved. Release the mouse over the landing zone and the widget will be moved.



- To move a widget to another Dashboard page, right-click on the widget menu button, which is located on the right-hand side of the widget's title bar, and select "Send to Page > Page Name". (Note: You may have to create an additional Dashboard page first.)
- To change a widget's configuration (including widget type), right-click on the widget menu button, which is located on the right-hand side of the widget's title bar, and select "Configure".

Widget Types

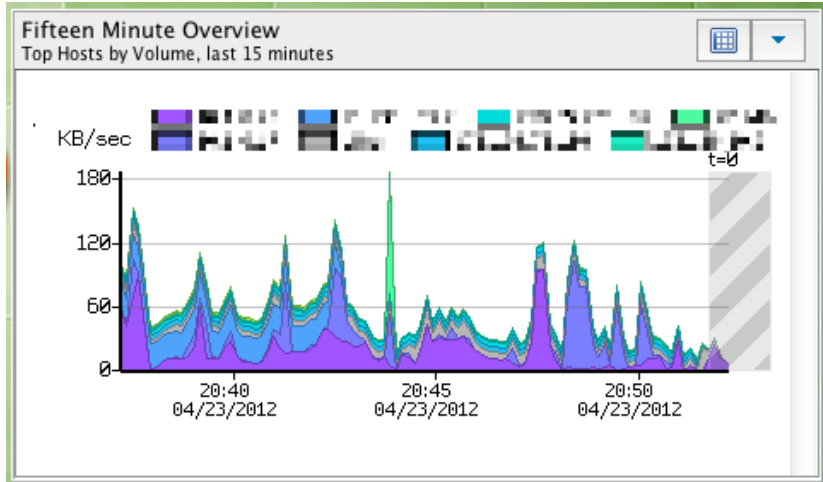
FlowTraQ has several types of widgets. In alphabetical order, they are:

Alerts

The *Alerts* widget provides an interface to FlowTraQ's alerting capabilities. It is discussed in more detail in the section called "Managing and Retrieving Alerts".

Charts and Tables

The *Charts and Tables* widget displays an automatically refreshed chart and table with a timeframe relative to now. Use it to get a quick overview of the activity of the last hour, day, or week. Each such widget represents the content of a single View (see the section called “Views”). You can specify a session filter (see the section called “Filtering”) and a refresh rate suitable to the interval displayed.

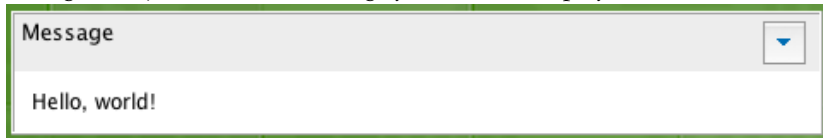


Flow Rate

The *Flow Rate* widget shows the total number of incoming flows processed by FlowTraq over time. It is discussed in more detail in the section called “The Flow Rate Widget”.

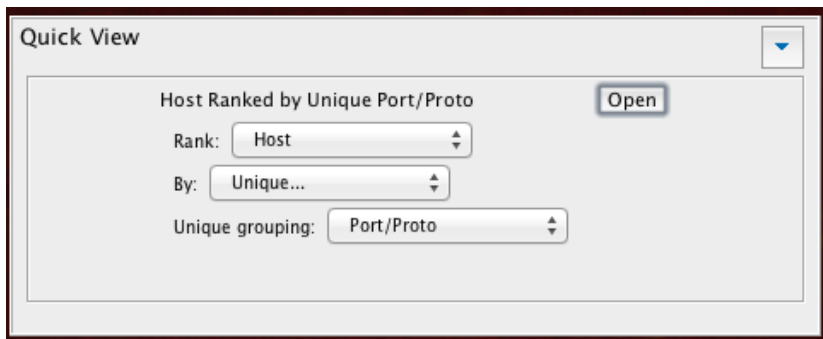
Message

The *Message* widget is designed to store useful text, like a sticky-note. To configure it, just write the message you wish to display.



Quick View

Use the *Quick View* widget to quickly launch a workspace showing a given view.



Reports

The *Reports* widget provides an interface to schedule and retrieve reports. It is discussed in depth in the section called “Managing and Retrieving Reports”.

Server Status

The *Server Status* provides a few key server statistics. It is discussed in depth in the section called “The Server Status Widget”.

Workspaces

The *Workspaces* widget provides an interface to manage and launch saved and built-in Workspaces. It is discussed in depth in the section called “Workspaces Widget”.

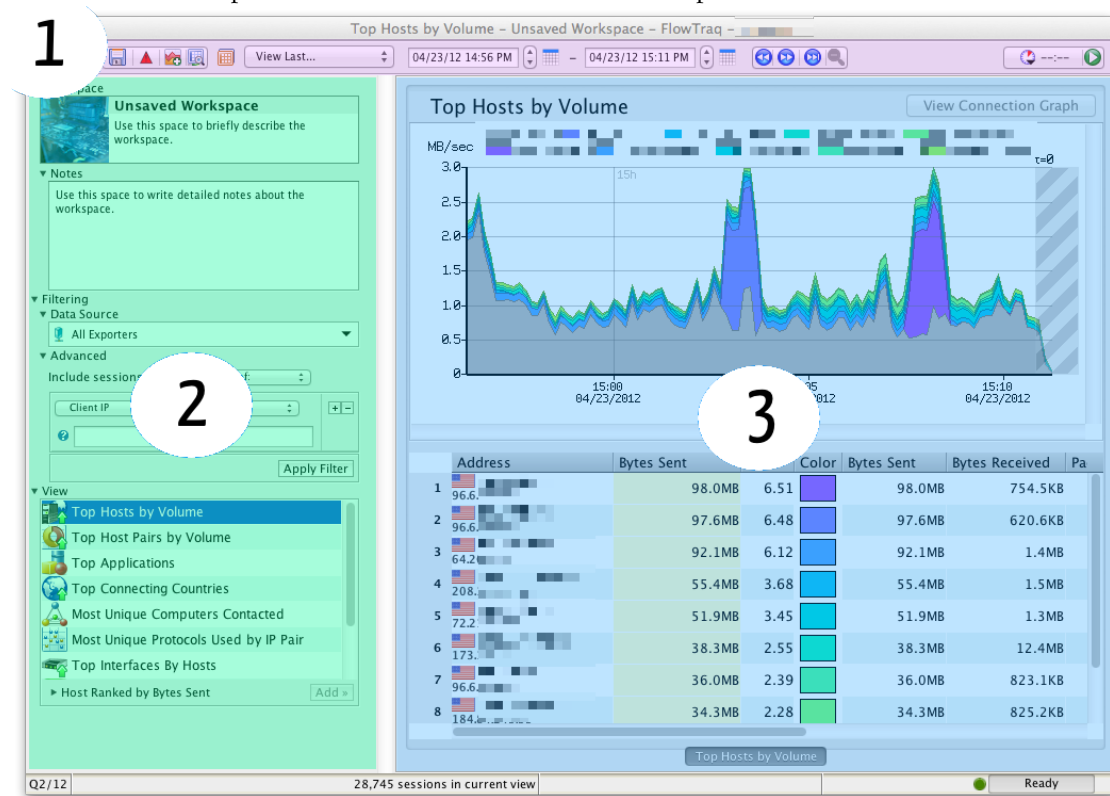
Chapter 8. Interactive Reports (Workspaces)

This chapter describes how to use FlowTraQ to perform interactive reporting and analysis via the Workspace window.

Workspace Overview

FlowTraQ Workspaces are interactive flow investigations. The Workspace user interface allows you to quickly build reports interactively by setting timeframes and filters at the click of a mouse and selecting views that show the statistics you are most interested in. The Workspace is designed with "pivoting" in mind; if you see something interesting in the data, interact with it to get a better view. For instance, you can drag mouse across a graph to zoom in on a timeframe of interest. Or, you can right-click on a row of a table to quickly filter on the corresponding host, country, application, or other entity.

These are just a few of the things you can do to quickly and interactively gain insight into your network traffic. This section provides a detailed overview of the Workspace window.



The Workspace window is organized into three major sections:

1. The toolbar, on top, includes all the timeframe navigation tools, as well as buttons to save a Workspace to the Dashboard, schedule the current Workspace as automated report, generate alert notifications based on the Workspace, open Session Explorer, and set up automatic refresh of the workspace.
2. The sidebar, on the left, includes the Workspace descriptions as well as all of the filtering and View selection controls.

3. The main data display shows the results of the current query. Session data is displayed in one or more *Views*, which are rankings of the session data displayed as a stack chart, a table, and (for pairwise rankings) an interactive connection graph which allows you to visualize connections between entities.

Example Workspaces

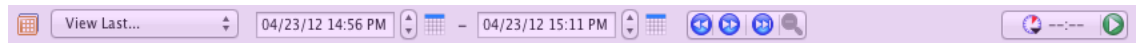
FlowTraq provides a variety of built-in Workspaces designed to demonstrate FlowTraq's flexible filtering capabilities. To launch one of them, find or create a Workspaces widget that is configured to show the Example Workspaces, and double-click one of the example Workspace's badges. A new Workspace window will launch.

Customizing Workspaces

To customize a Workspace, begin by launching either an example Workspace (see above) or a new Workspace (select the "New Workspace" button from the Dashboard toolbar or select *File > New Workspace* from the Workspace menu).

Once a Workspace window is open, you can customize the timeframe, filter, and Views by using the controls in the time navigation toolbar and the sidebar.

Time Navigation



The time navigation toolbar allows you to quickly select commonly used timeframes, specify a time and date range you are interested in, and navigate forward and backward to the previous or next time segment. This toolbar also allows you to configure automatic refreshing.

To quickly specify a timeframe relative to the current time, use the first two controls on the toolbar: the *Time Selection Mode* toggle button and the *Time Selection* dropdown. Use the toggle button to select either the *View last...* or the *Fixed Frame* modes, and then use the dropdown to select a timeframe.

Tip

Both the *View last...* and the *Fixed Frame* modes select time frames relative to the current time, and can be used with the auto-refresh, which will refresh the screen with new data at regular intervals.

By default, the time selection method is *View last...*. In this mode, the dropdown will show options for the last *15 minutes*, *30 minutes*, *1 hour*, *3 hours*, and so on. Selecting any of these will cause the workspace to refresh to the selected time segment.

In *Fixed Frame* mode, the dropdown contains options for *this hour*, *last hour*, *today*, *yesterday*, and so on.

Tip

If you prefer to specify a timeframe by hand, use the start and end time boxes and spinner controls to specify the times you're interested in. Enter a date, or use the Calendar popup button to quickly navigate to relevant dates. Finally, after entering your timeframe, click the *Refresh* button to retrieve the data. If you specify a timeframe by hand, any selections you have already made in the Time Selection dropdown are ignored.

You can navigate to the previous or the next segment in time using the *Forward* and *Backward* buttons on the right side of the time navigation bar, and you can quickly move the timeframe so that it ends at the current time by pressing the *Forward To Now* button.

Finally, in the data display, you can zoom in by dragging the mouse across the graph while holding down the left button. This will zoom in on the selection region and refresh the data automatically.



Long-Running Sessions

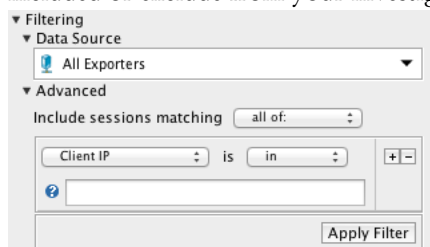
When a session overlaps the selected timeframe but the start time is before the start of a time frame, or end time is after the end of a time frame, that session's statistics are pro-rated to the timeframe. That is, suppose hosts are being ranked on bytes transferred, and a host has a session that is 50% in the selected timeframe, and 50% out of it; in this case, only half the bytes in the session are counted to that host.

Filtering

FlowTraq offers extensive and powerful filtering capabilities. Filters can be configured in the Workspace sidebar, in the Report Scheduler, and in the Alert Scheduler. In all three cases, filters are configured in the same way.

Building Filters

Generally speaking, you configure a filter by combining constraints which specifies which traffic to included or exclude from your investigation. The Filtering panel looks like this:



The first constraint you can specify is the data source selection. If you may have more than one flow source reporting flows to FlowTraq Server, you may use the Data Source dropdown to select an exporter or a particular interface on an exporter to use as the data source. (You can also keep the default setting, "All Exporters"). If you choose an exporter or an interface, subsequent reports will include only traffic that was reported by that device, or which passed through that interface.

Subsequent constraints are specified in the Advanced Filter panel. You can form these constraints as easily as you can form English sentences by selecting from dropdowns and completing the fields in a filter box, which is sometimes referred to as a *Filter Line*. You can also add and remove Filter Lines as you see fit by clicking on the '+' and '-' buttons on each Filter Line.

Most Filter Lines can accept comma-separated sets of host names, CIDR blocks, numeric ranges, or mnemonics (such as "tcp" for protocol), as appropriate to their type. Others, such as the country code selector, provide an interface that allow you to select values. All Filter Lines have a validation icon which indicates if the value entered has been accepted. When you start typing, the validation icon turns into a question mark. When the icon turns green, the filter box value has been accepted and can be applied. If the icon turns red, you have entered an invalid value for the Filter Line, and your input on that Filter Line will be ignored. (You can click the validation icon for an explanation of why your input was rejected.)



Combining Filter Lines

By default, Filter Lines are combined by logically "AND"-ing them together. That is, if you specify the following three Filter Lines: *A*, *B*, & *C*, only sessions for which *A AND B AND C* are true will be included in the report.

If you'd like to "OR" them together, change the *Combination Rule* by changing the dropdown in the that says "Include sessions matching ALL of:" to say "Include sessions matching ANY of:".

Values entered into a particular Filter Line are combined by logically "OR"-ing them together.



Filtering Example 1

If you want to filter on traffic (to or from) either 172.16.2.2 OR 192.168.12.12, use this filter:

▼ Advanced

Include sessions matching all of:

Either IP is in + -

172.16.2.2, 192.168.12.12

Apply Filter

Instead, if you want to filter on traffic between the two addresses (that is, both 172.16.2.2 and 192.168.12.12 are part of the session, but without regard to which is the client and which is the server), then use this filter:

▼ Advanced

Include sessions matching all of:

Either IP is in + -

172.16.2.2

Either IP is in + -

192.168.12.12

Apply Filter

And if you would only like to see traffic where 192.168.12.12 is the server, and 172.16.2.2 is the client, use this filter:

▼ Advanced

Include sessions matching all of:

Client IP is in + -

172.16.2.2

Server IP is in + -

192.168.12.12

Apply Filter

Now, if you want to see traffic that went to either 172.16.2.2 OR 192.168.12.12, used protocol TCP, and went to server port 80 (HTTP), then try this filter:

▼ Advanced

Include sessions matching

Either IP in
☒ 172.16.2.2, 192.168.12.12

Protocol any of
☒ TCP

Server Port any of
☒ 80

Filtering Example 2

In some cases you might want to OR the filter boxes. For instance, suppose your accounting division uses VLAN 5, and the accounting database server is 192.168.12.33. You want to filter on *all* accounting traffic. In this case you set the combination rule to be "Include sessions matching ANY of:"

▼ Advanced

Include sessions matching

VLAN (Either) any of
☒ 5

Server IP in
☒ 192.168.12.33

This filter includes all traffic on VLAN 5, regardless of destination or protocol, and all traffic going to the accounting server.

Filtering Example 3

Suppose you have a dedicated VLAN for your IP phones (say, VLAN 6), but you suspect that some of the phones may have been misconfigured and are using bandwidth on the regular bulk data network. The filter to detect this behavior will have to *exclude* the VOIP VLAN but *include* all non-bulk TOS traffic to the VOIP servers (say, in the 69.59.241.0/24 class-C block).

A filter to find all your rogue VOIP phones might look like this:

▼ Advanced

Include sessions matching

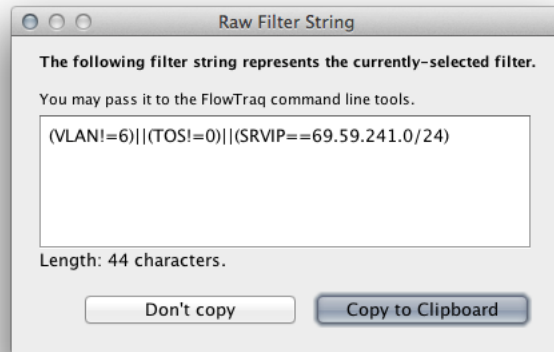
VLAN (Either) none of
☒ 6

ToS/DiffServ none of
☒ 0

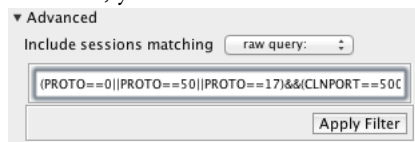
Server IP in
☒ 69.59.241.0/24

Raw Filter Strings

You can view the raw filter string corresponding to a set of Filter Lines by selecting *View > Filter String*:



You can use the raw filter string on the command line, or as a starting point for more complex filter strings. If you find that you cannot fashion the filter you need to using the Filter Line interface, you can enter a raw filter string by selecting "raw query:" as the Combination Rule:



See the section called “Filter String Syntax” for more information on the filter language syntax.

Filter Fields

Below is the full list of fields that can be filtered on:

IP address/hostname/CIDR block	The most common filter is a host filter or address block filter. You may specify client, server, or both. This is useful, for instance, if you want to find all inbound connections to your web server, but are not interested in outbound connections that the web server initiates itself. Valid inputs are IPv4 addresses in dotted-decimal notation; IPv6 addresses; hostnames (be sure to wait for the validation icon to indicate the name was successfully resolved); and CIDR blocks (both IPv4 and IPv6). CIDR blocks are a convenient way of specifying an entire subnet; for example, use 192.168.12.0/24 to include all addresses from 192.168.12.0 to 192.168.12.255.
MAC Address	Filter on the MAC addresses in the session, as reported by the exporter (IPFIX fields 56 and 80).
Port	Filter on the port number. It is possible to specify a range of ports by choosing between ; enter ranges using a dash. For example, selecting between with a value of "10000-20000" will find all sessions with port numbers between 10,000 and 20,000.
Protocol	Filter on a protocol. Accepted mnemonics are TCP, UDP, and ICMP. Numeric protocol values are also allowed.

Country Filter on sessions to or from a particular country. Click the "Edit" button to get a list of countries, and select countries to include in the filter by toggling their country-code button. A list of selected countries and their flags will appear in the Filter Line.

Bytes Filter on session byte volume. For instance, if you only want to view sessions where the client sent at least 500 bytes, then select "Client Bytes", "at least", and supply the value "500" in the input field.



Important

Selecting "Either Bytes" does NOT sum the client and server-side bytes together. Rather, it acts as a logical OR. Use "Total Bytes" to filter on the total bytes.

Packets Filter on session packet volume. In all ways analogous to Bytes.

ToS/DiffServ Filter sessions based on the value in their ToS or DiffServ field. The values are numeric, so you might need to specify a range to get the desired effect.



Important

Note that this field has a different meaning for IPv4 and IPv6.

Flow Duration Filter sessions based on their duration. This field is numeric and given in seconds.



Tip

From a security perspective, it may be useful to filter on particularly long-lived connections. To do so, select the "at least" option and supply a value of 7200 in the input field to include only sessions that lasted at least 2 hours.

VLAN Filter on the session's VLAN numbers.

VLANs are a convenient way to group classes of systems together. VLAN specifiers are numbers between 1 and 4096. Most sessions will have the same VLAN ID for both VLAN In and VLAN Out. Devices that route packets between VLANs will export flows where the VLAN In and VLAN Out differ. When VLANs are not used, this value is commonly set to 0.



Exporter VLAN Support

Not all flow sources include VLAN information in their flow updates. In particular, NetFlow v5 does not include VLAN information, and some versions of cFlow, and jFlow also do not.

ASN Filter on the session's Autonomous System Numbers. Some routers keep BGP tables to make routing decisions at the au-

	onomous system level. These routers may include the ASN of the client and the server address in the flow records. You can use this option to filter on this field.
Interface	Filter on the exporter-reported Interface In and Interface Out numbers of the session. This serves a similar function to the feature provided by the Data Source selection box. Use this if you want to filter on more than one interface, but not all interfaces. Interface numbers range from 1-65536. A value of 0 indicates no interface number was present in the flow records.
Exporter IP	Filter on the IP address of the exporter which reported the session. This serves a similar function to the feature provided by the Data Source selection box. Use this if you want to filter on more than one exporter, but not all exporters.
Exporter Version	Filter on the NetFlow/sFlow version of the exporter which reported the session. Click the "Edit" button to get a list of versions, and select versions to include in the filter by toggling their buttons. A list of selected versions and their badges will appear in the Filter Line.
NSEL Event	Filter on the NSEL event code of the session. Typically, NSEL events correspond to a flow being accepted, denied, or deleted by the firewall. Click the "Edit" button to get a list of event codes, and select event codes to include in the filter by toggling their buttons. A list of selected event codes and their numbers will appear in the Filter Line.
NSEL Ext. Event	Filter on the NSEL extended event codes of the session. Typically, NSEL extended event codes explain why a flow was denied by the firewall. Click the "Edit" button to get a list of event extended codes, and select event codes to include in the filter by toggling their buttons. A list of selected event codes and their numbers will appear in the Filter Line.

Views

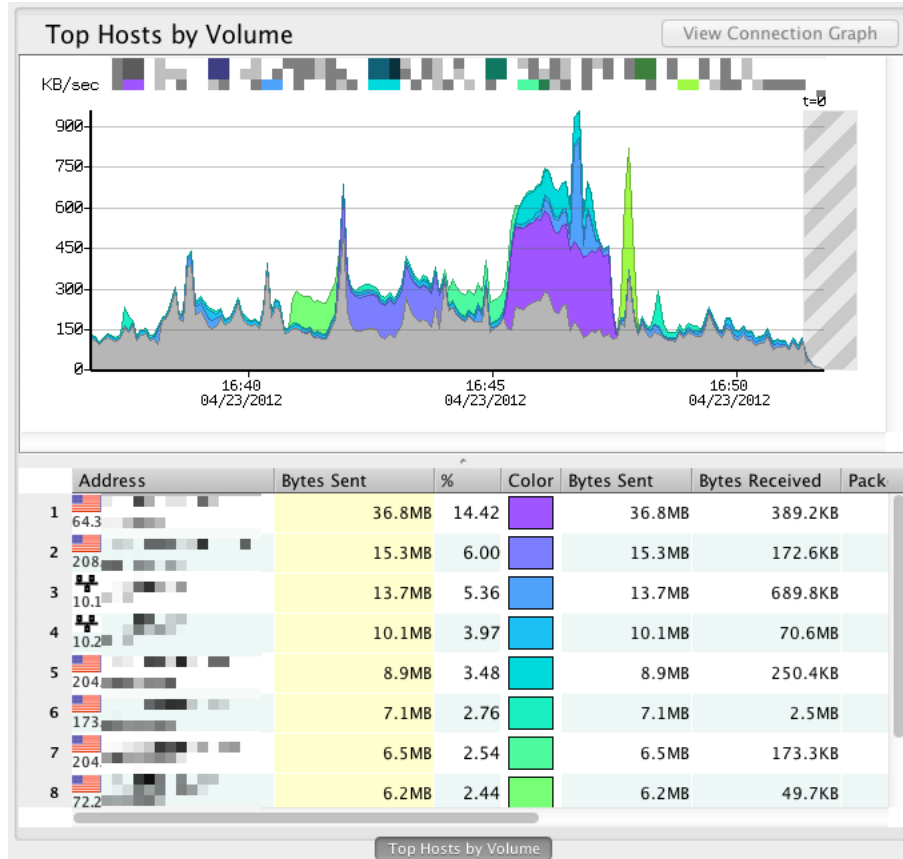
FlowTraq has the ability to rank your selection of traffic in hundreds of different ways. Each such ranking is called a *View*. Being able to analyze traffic from multiple angles often reveals unexpected details, so Workspaces can show many Views at once, in tabs.



Important

You must have add least one View to the Workspace before you can retrieve and analyze traffic.

In general, each View consists of a stack chart and a table which serves as a legend for the stack chart. Stack charts are a convenient way to visualize ranked data over time. The top-ranked item appears at the bottom of the graph; stacked on top of it is the second-ranked item; and so forth:



The grayed-out crosshatch area on the chart roughly indicates the present time. More specifically, it indicates when insufficient flow data has been received to compile a completely accurate representation of the traffic. In general, the crosshatch area starts at about 60 seconds into the past, and extends indefinitely into the future.

Tables show the same data as the chart above them, but in a sortable table format. In fact, you can click on any part of the chart and FlowTraq will highlight the corresponding row in the table below.

Tip

Use the *View > Top-10*, *View > Top-25*, ..., *View > Top-1000* items in the Workspace menu to indicate how many rows FlowTraq should include in its rankings.

You can right-click on any item in the table to see contextual options (for instance, you can add an item to your session filter).

You can also change the widths of the columns and rearrange columns for your convenience. (This setting is remembered on a user-by-user basis.)

By default, the second column in the graph is highlighted. This is the column that was used to perform the ranking. In the example, above the data was sorted based on the number of bytes sent by each host. This means that the items in the table are the top hosts, ranked by bytes sent.

The columns further to the right give additional insight into the top hosts.



Important

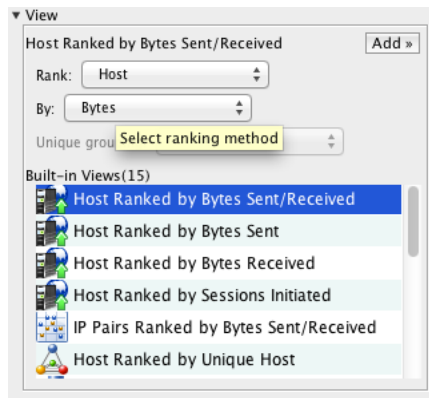
Although you can sort by the non-highlighted columns, they do not constitute a ranking by themselves. That is, if you re-sorted the above table by "Sessions Initiated," you will see the hosts that initiated the largest number of sessions *that also happened to make it into the original ranking*, which was "Top Hosts by Bytes Sent." In order to make a "Top Hosts by Sessions Initiated" ranking, you must add a new View in a separate tab. This is described below.



Tip

Pairwise Views can also be visualized as Connection Graphs. See the section called "The Connection Graph" for more information.

Built-in Views

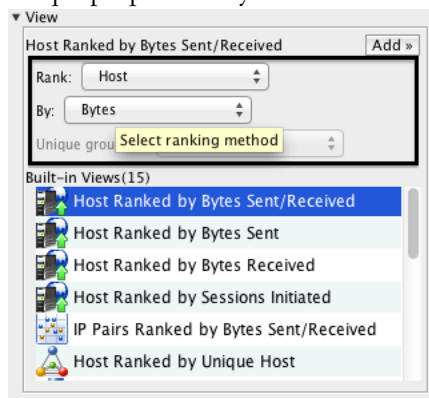


FlowTraq provides a number of built-in Views, which represent the most frequently used rankings.

To add a built-in View to a Workspace, select it from the View table and select "Add".

Custom Views

Built-in Views only scratch the surface of FlowTraq's capabilities. Use Custom Views to explore the unique properties of your network.



To define a custom view, select "Custom View..." in the View table, make your selections using the dropdown menus which appear, and click "Add" to add the view as a tab in the workspace.

Views are defined by selecting what entity to *Display* (or rank), and what aspect of that entity to rank. For instance, "Display: VLAN Ranked by Packets" will show you the top VLANs based on the number

of packets that were seen on that VLAN during the specified timeframe. On the other hand, "Display: VLAN Ranked by Bytes" will show the top VLANs based on the number of bytes seen. You may get a completely different ranking, because the byte volume of traffic can differ significantly from the packet volume on a given VLAN.

Tip

Take some time to familiarize yourself with the *pairwise* View (such as rankings of IP pairs) and *unique-count* Views (such as "Top Hosts Ranked by Unique Host"), as they are among the most powerful kinds of Views.

Defining your own View can be a powerful way to explore your traffic.

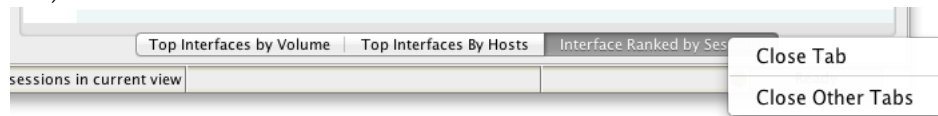
View Tabs

Each View you add to a Workspace becomes a tab in the data display. Select the tab to show that View in the display.

View Tab Limitations

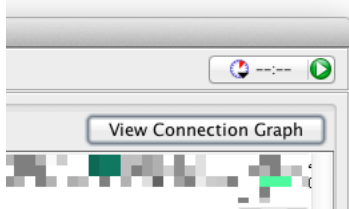
You can add up to ten concurrent Views in the data display. In addition, there are certain rules about which Views can be combined with which other Views. For instance, you can only add 2 View tabs that rank hosts or host pairs. If you attempt to add a View tab when either the maximum number of View tab has already been added, or a conflicting set of View tabs has already been added, the "Add" button will be disabled. This limitation is imposed to limit the memory usage by the server during query processing, and can be worked around by creating a second similar workspace, or by removing one or more View tabs before proceeding.

To remove a View, right-click on the View tab and select "Close Tab" to remove it. (Alternatively, select "Close Other Tabs" to remove all Views *except* the one represented by the selected tab.)

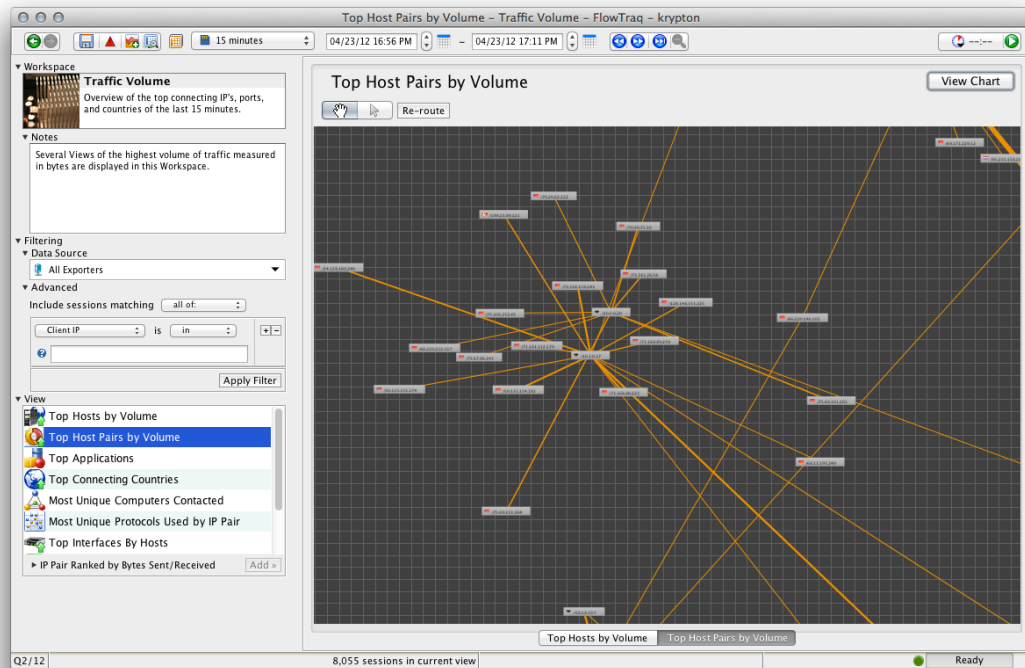


The Connection Graph

When a pairwise View is the active tab, a button labeled "View Connection Graph" is available in the upper right-hand corner of the data display:



Use this button to toggle between the chart/table display and the Connection Graph:

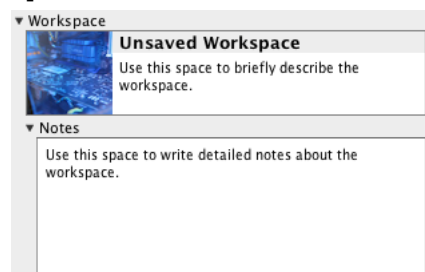


In Connection Graph mode, entities are displayed as badges with lines indicating connections between them.

To navigate the Connection Graph, click the "Hand" icon and drag the mouse within the graph, and zoom in and out using the mouse wheel or trackpad scroll gesture.

To interact with entities on the Connection Graph, click the "Cursor" icon, and then click or drag to select entities or groups of entities. Once selected, entities can be rearranged by dragging, or right-clicked to present a contextual menu.

Workspace Details



FlowTraq provides you with spaces in the sidebar to briefly describe your Workspace and make notes to remind you of the status of your investigation. Feel free to use these spaces in ways you find appropriate.

In addition, you may select a Workspace icon to help you quickly identify your Workspace in the Workspaces widget. To do so, click on the icon in the Workspace badge and an icon chooser will appear:



Click on the desired icon to select it.

Saving and Sharing Workspaces

FlowTraq provides several options for saving Workspaces.

1. You can save a Workspace to your user Dashboard and access it later via a Workspaces widget.
2. You can export a Workspace to disk as a .ws file, which can be shared and re-imported via the Dashboard. You may find this useful for sharing your Workspaces with others in your organization.



Important

Note that saving a Workspace stores the timeframe, filter, selected Views, your description and notes, and name of the Workspace. It does *not* store the *results* of a particular report, but rather the *information needed to re-run a report later*.

To save an interactive report's actual results, please export a PDF, or print the results (see below).

To save a Workspace to your Dashboard, use the "Save" button on the toolbar, or select *File > Save Workspace* from the Workspace menu.



Important

If you are saving a Workspace for the first time, you will be prompted to name your Workspace.

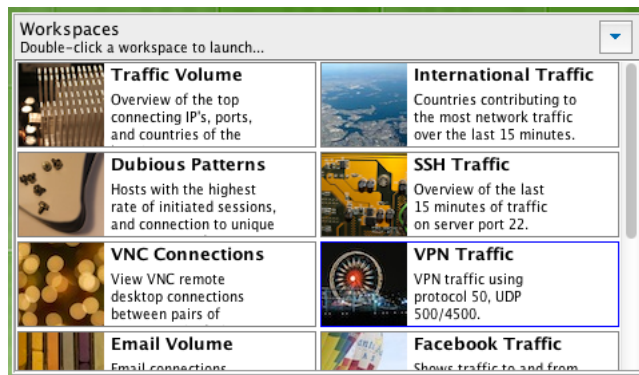
The Workspace's details will be stored on FlowTraq Server, and will appear on your Dashboard in a Workspaces widget.

Importing and Exporting Workspaces

Like saving a Workspace to your Dashboard, exporting a Workspace saves the Workspace's configuration but not the results.

- To export a Workspace to disk, select *File > Export Workspace...* from the Workspace menu.
- To import a Workspace, select *File > Import Workspace...* from the Dashboard menu.

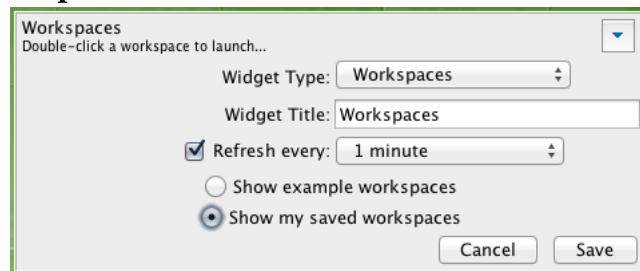
Workspaces Widget



When you save a Workspace, it will appear as a badge in a Workspaces widget on your Dashboard. From there, you re-open saved Workspaces.



Important



The Workspaces widget has two modes. In one mode, it shows a built-in set of Example Workspaces. In the other, it shows your saved Workspaces. If you do not have a Workspaces widget on your Dashboard that is configured to show your saved Workspaces, you must create one in order to re-open your saved Workspaces.



Tip

You can also delete saved workspaces by right-clicking them and selecting the appropriate menu item.

Printing and Saving Interactive Reports

To save an interactive report's actual results, FlowTraq provides two options:

1. You can print the report. To do this, select *File > Print Report...* from the Workspace menu, and follow the on-screen instructions.
2. You can export a PDF of the report. To do this, select *File > Export PDF...* from the Workspace menu and choose a file name and location.

Chapter 9. Scheduled Reports

FlowTraq's full-fidelity flow database allows you to generate reports at any time without having to concern yourself with whether the source information is still available: as long as the session database's maximum size is large enough, FlowTraq will maintain the historical record indefinitely without aggregation.

Important

When the session database has reached its maximum size, FlowTraq will remove the oldest records first. For more information on the session database, see the section called “The Session Database”.

While it is useful to be able to interactively generate reports after-the-fact, some reports take longer to perform than others. For instance, it may take minutes or hours to generate a report with a one-month or one-year timeframe. In particular, if the records needed to perform a query are on disk, rather than in FlowTraq's memory cache, generating reports interactively might be prohibitively slow.

Additionally, you might simply want to see the same data at regular intervals.

For these kinds of situations, FlowTraq has a flexible report scheduling function. Any kind of report which you can generate interactively in a Workspace can also be scheduled to run automatically and regularly and retrieved from the Dashboard for viewing, printing, or saving to PDF.

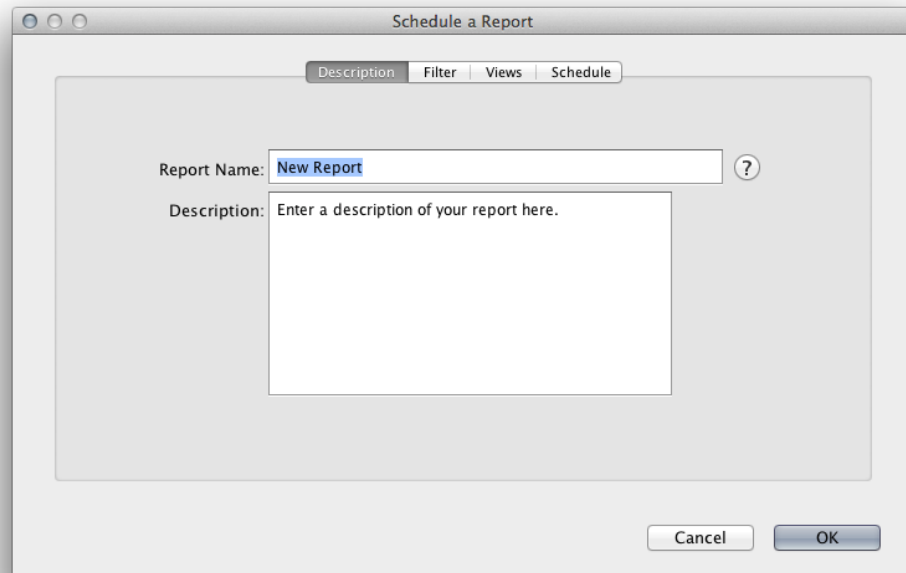
This chapter describes how to schedule, retrieve, and manage scheduled reports.

Scheduling Reports

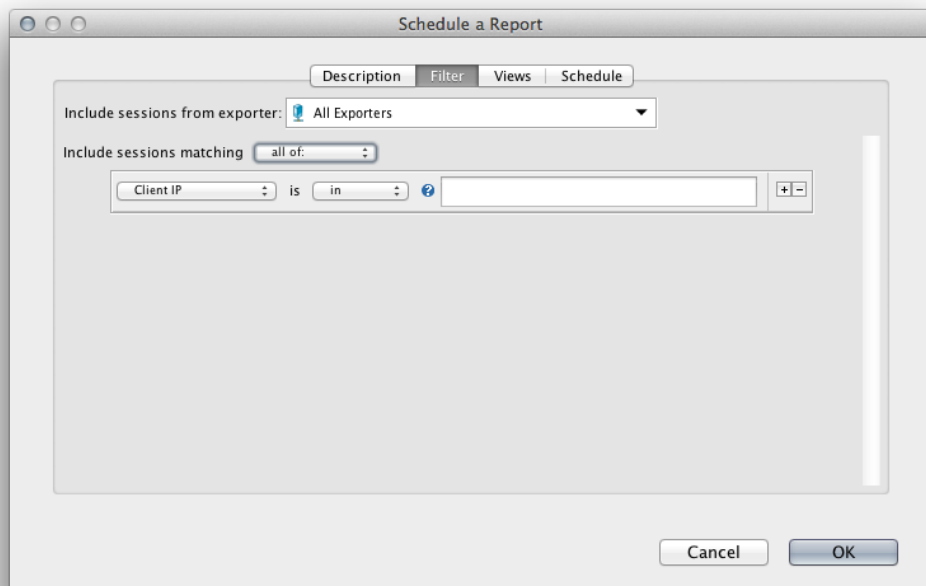
Reports are scheduled using FlowTraq Client, but the report schedule is stored by, and performed by, FlowTraq Server. This means FlowTraq Client does not have to be running in order for reports to be generated; in other words, if you schedule a report to run every day at midnight, and then you close FlowTraq Client and go home for the day, the results of that report will be waiting for you the next time you log in to FlowTraq.

To schedule a report, take the following steps.

1. Access the "Schedule a Report" window. There are two ways to access it:
 - From within a Workspace window: click the "Schedule Current Workspace As Report" button on the toolbar.
 - From the Dashboard: right-click an empty row of a Reports widget and select "Schedule New Report".
2. On the "Description" tab, title your report and, optionally, provide a brief description.



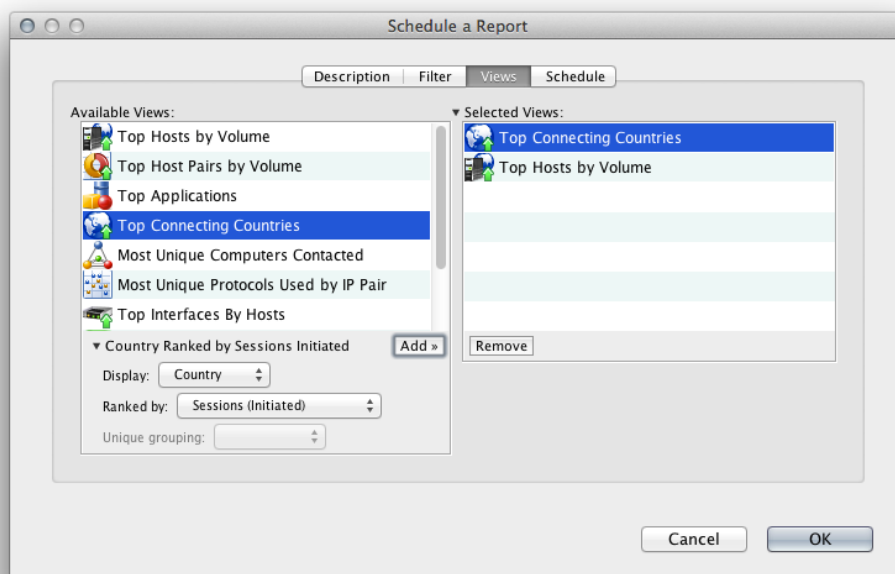
3. On the "Filter" tab, set the session filter you would like to be applied when generating the report.



Tip

If you accessed the "Schedule a Report" window from a Workspace, the session filter you specified there will be carried over into the report.

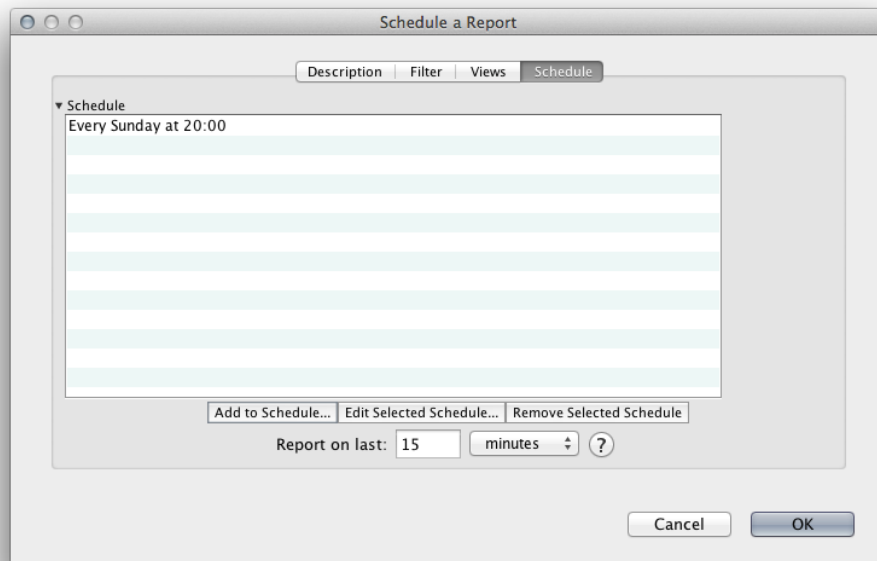
4. On the "View" tab, select the Views you want to be included in the report. Click "Add" on the left-hand pane to add a view to the right-hand pane.



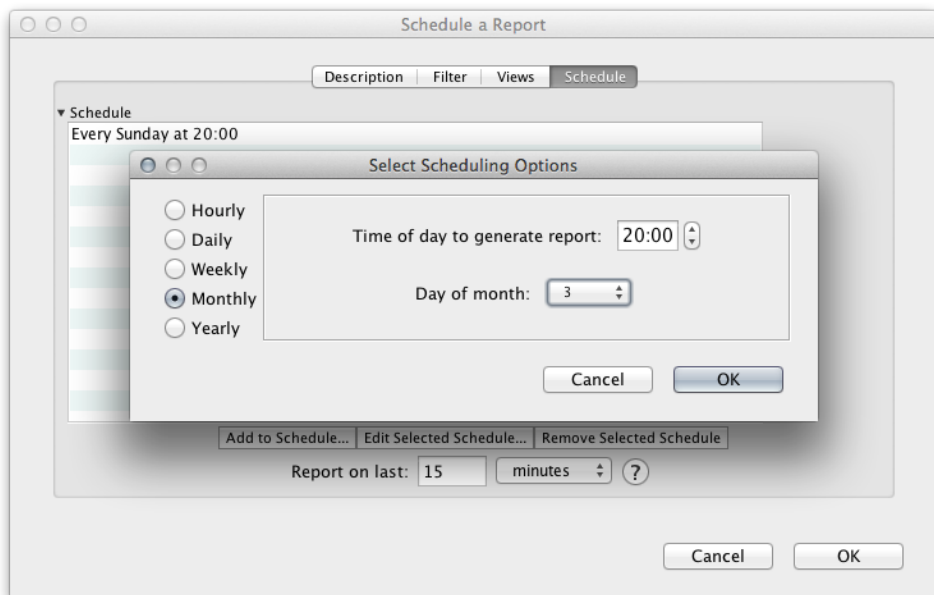
Tip

If you accessed the "Schedule a Report" window from a Workspace, any Views you have selected there will be carried over into the report.

5. On the "Schedule" tab, configure when the report will run and the desired report duration.



To configure when the report will run, click the "Add to Schedule..." button and, in the window that appears, choose how frequently you want the report to run (hourly, daily, weekly, monthly, or annually) and at what time of day (or day of week, etc) you want it to run.



 Tip

You can add more than one line to the schedule. This allows you to configure the report to run at a variety of times.

After configuring *when* the report will run, enter the desired report duration by completing the *Report on last:* field. This determines the timeframe over which the report will be generated.

 Example

To generate a report for the 9am-5pm timeframe of each work day (Monday through Friday) at the end of the work day, you must add five lines to the schedule: One for each Monday; one for each Tuesday; and so on.

Add a line to the schedule, and select *Weekly*, then *Monday*. Set the time to 17:00.

Repeat this four more times for the other four days of the week.

Finally, in the "Report on last:" entry, enter *8 hours*.

FlowTraq will generate a report of each work day's traffic automatically at the end of the work day.

6. Click "OK" and the report will be scheduled.

Managing and Retrieving Reports

The Reports widget provides the interface for retrieving and managing scheduled reports. To add a Reports widget to your Dashboard, create it as you would any other widget. (See Chapter 7, *The Dashboard* for more information on managing the Dashboard.)

The Reports widget has two modes:

- *Show Generated Reports*. In this mode, the Reports widget displays the list of generated reports. Suppose one week ago you scheduled a report to run every day at midnight. In this mode, the Reports widget would display seven rows, each of which represent the results of a single run of that report.
- *Show Report Schedule*. In this mode, the Reports widget displays the list of report types you have scheduled. Suppose one week ago you scheduled a report to run several times a day. In this mode, the Reports widget would display only one row, representing that scheduled report.

To toggle between these modes, click the toggle button, which is the first button on the widget's title bar.

Editing, Disabling, and Deleted Scheduled Reports

To edit, disable, or delete an already-scheduled report, take the following steps:

1. Put the Reports widget in *Show Report Schedule* mode.
2. To edit a report, double-click on the report you want to edit, or right-click on it and select "Edit Report Schedule." The "Schedule a Report" window will appear. Make the desired changes to the report's description, filter, views, or schedule, and click OK to save your changes.

To disable or delete an alert, right-click on the alert you want to disable or delete and select the appropriate item from the context menu.

Retrieving Reports

You can retrieve the result of a scheduled report and view it in a window, send it to a printer, or save it as a PDF. To do so, take the following steps:

1. Place the Reports widget in *Show Generated Reports* mode.
2. To view the results of a report in FlowTraq, double-click on the report you want to retrieve and a window will appear. Alternatively, to print or save the results, right-click on the report and select "Print Report" or "Save Report."

Deleting Generated Reports

The results of reports are stored on FlowTraq Server and are very compact. Still, over time you may find that your Report widget lists reports that are no longer useful to you. To delete one or more reports, take the following steps:

1. Place the Reports widget in *Show Generated Reports* mode.
2. Select one or more generated reports. You can select more than one by using the Shift key (to select a range) or the Command/CTRL key (to select several non-contiguous reports).
3. Right-click on the selected report or reports and select "Delete Report(s)", and confirm your selection in the dialog box that follows.



Caution

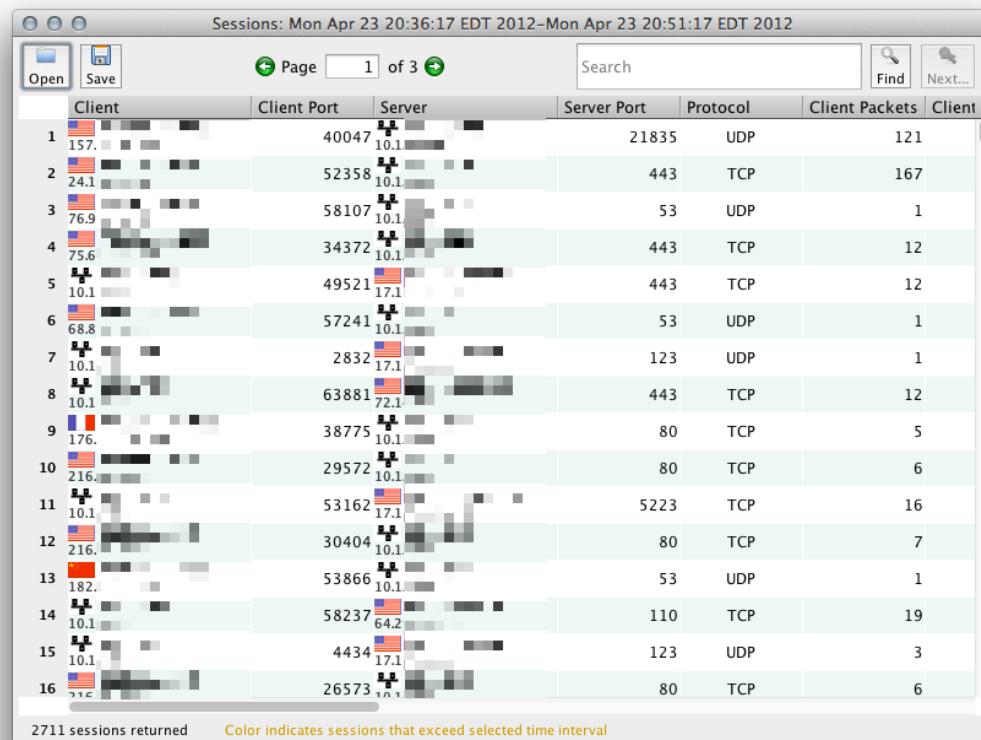
You cannot undo this operation.

Chapter 10. Session Explorer

One of the most powerful and unique features of FlowTraq is the efficient storage of flow records with full fidelity. This technology lies at the foundation of FlowTraq's capability to flexibly and quickly generate arbitrary reports.

It also enables you to view the actual session records collected FlowTraq, which allows you to isolate individual sessions or export sets of sessions for your own analysis.

Session Explorer provides the interface for viewing, searching, sorting, and saving session records.



The screenshot shows the Session Explorer window with a title bar indicating the time range: "Sessions: Mon Apr 23 20:36:17 EDT 2012–Mon Apr 23 20:51:17 EDT 2012". The interface includes a toolbar with "Open", "Save", "Page 1 of 3", a search bar, and "Find", "Next..." buttons. The main table displays session records with columns: Client, Client Port, Server, Server Port, Protocol, Client Packets, and Client. The table contains 16 rows of data, each representing a session. The status bar at the bottom indicates "2711 sessions returned" and "Color indicates sessions that exceed selected time interval".

	Client	Client Port	Server	Server Port	Protocol	Client Packets	Client
1	157.	40047	10.1	21835	UDP	121	
2	24.1	52358	10.1	443	TCP	167	
3	76.9	58107	10.1	53	UDP	1	
4	75.6	34372	10.1	443	TCP	12	
5	10.1	49521	17.1	443	TCP	12	
6	68.8	57241	10.1	53	UDP	1	
7	10.1	2832	17.1	123	UDP	1	
8	10.1	63881	72.1	443	TCP	12	
9	176.	38775	10.1	80	TCP	5	
10	216.	29572	10.1	80	TCP	6	
11	10.1	53162	17.1	5223	TCP	16	
12	216.	30404	10.1	80	TCP	7	
13	182.	53866	10.1	53	UDP	1	
14	10.1	58237	64.2	110	TCP	19	
15	10.1	4434	17.1	123	UDP	3	
16	216.	26573	10.1	80	TCP	6	

Accessing Session Explorer

There are two way to access Session Explorer.

- From a Workspace, you can retrieve the sessions that match the active timeframe and filter and open them in Session Explorer. To do this, take the following steps:
 1. Open a Workspace and use the Time Navigation toolbar and Filter sidebar to select sessions of interest. (For more information on Time Navigation and Filtering, see the section called “Time Navigation” and the section called “Filtering”).
 2. Click the *Fetch All Sessions* button from the Workspace toolbar.



Important

Session Explorer will immediately start downloading matching sessions using the filter and timeframe you currently have defined in the Workspace. If there are millions of sessions in your current view, this may take some time.

- To import a session record that you previously saved from within Session Explorer, select the *Import Sessions* button from the Dashboard toolbar, or select *File > Import Sessions...* from the Dashboard menu.

Session records contain a number of fields, including the IP addresses of the client and the server in the conversation, information about the exporter which reported the session, TCP flags (if applicable), the country of each address, server and client port numbers (for TCP and UDP), VLAN IDs, and timestamps of the start and end of the session.



Long-Running Sessions

When a session overlaps the selected timeframe but the start time is before the start of the selected timeframe, or end time is after the end of the selected timeframe, that session is *included* in Session Explorer, but start times and/or end times are marked in yellow to indicate that the session is partially outside the selected timeframe.

Note that, in contrast to the rankings generated by FlowTraq, the information in raw session records is *not* pro-rated to the selected timeframe.

Using Session Explorer

- To sort on any of the session fields, click on the appropriate column header.



Important

If Session Explorer is showing a large number of records, it may take some time to sort them.

- Records are paginated in sets of 1000. To navigate pages, use the left and right arrows in the toolbar. Alternatively, enter a page number.
- To search the session records, enter your search term in the *Search* bar and use the *Find* and *Next...* buttons.



Tip

Press ENTER key in the *Search* field as a shortcut to the *Find* or *Next...* buttons.

- To save session records to disk, select *File > Save* from the Session Explorer menu, or click the *Save* button.



Tip

Session records are saved in CSV format. They can be opened in Session Explorer or any other application that supports the CSV format.

Chapter 11. Alerts and Notifications

FlowTraq is able to generate alert notifications in real time based on user-specified conditions. When such a condition is met, FlowTraq is able to generate notifications of alert conditions in several ways:

- Alert notifications are displayed in an Alert widget on the Dashboard of the user who set the condition.
- Alert notifications can optionally be e-mailed to the user who set the condition.
- Alert notifications can optionally be sent via syslog over UDP for integration with third-party SIEM (security information and event management) systems.
- Alert notifications can optionally be retrieved via the command line for scripting.

An *alertable condition* (or simply alert condition) is a time-based threshold set on any metric which can be calculated using network flows. For instance, "number of sessions initiated by any one host exceeds one thousand over a period of thirty minutes" is an alertable condition. If it is set, FlowTraq will track the number of sessions initiated by all hosts, and at any time, if a host initiates more than one thousand sessions over the course of two minutes, FlowTraq will notify the user who set the alertable condition.

In addition, FlowTraq allows you to specify a prefilter to indicate what kinds of sessions to include when tracking for a given alertable condition. The prefilter is configured in the same way as report filters.

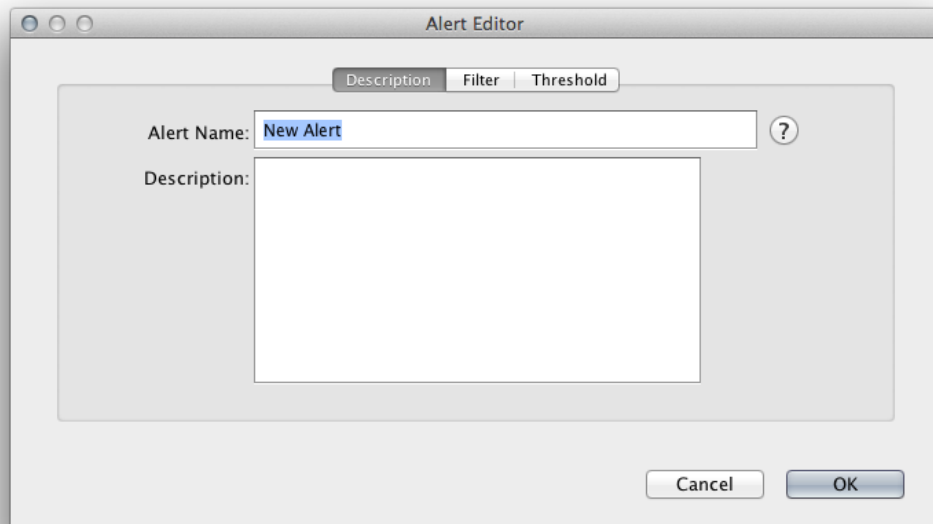
This chapter describes how to configure, retrieve, and manage alerts.

Setting Up Alerts

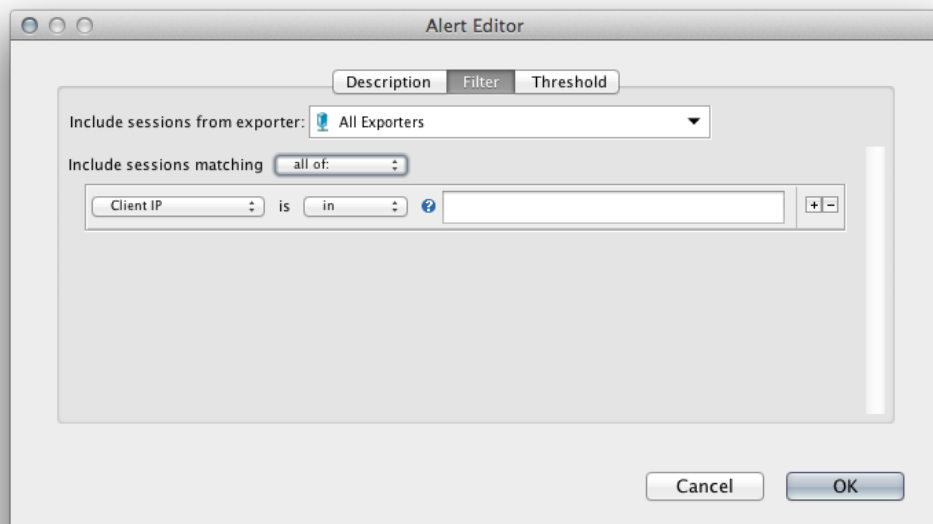
Like reports, alerts are configured using FlowTraq Client, and like reports, the list of alerts is stored by FlowTraq Server. Also, FlowTraq Server is responsible for generating notifications. This means FlowTraq Client does not have to be running in order for alert notifications to be generated; in other words, if you set an alert and then close FlowTraq Client, notifications will still be generated whenever the alert's condition is met.

To configure an alert, take the following steps.

1. Access the "Alert Editor" window. There are two ways to access it:
 - From within a Workspace window: click the "Alert" button on the toolbar.
 - From the Dashboard: right-click an empty row of an Alerts widget and select "Schedule New Alert".
2. On the "Description" tab, title your alert and, optionally, provide a brief description.



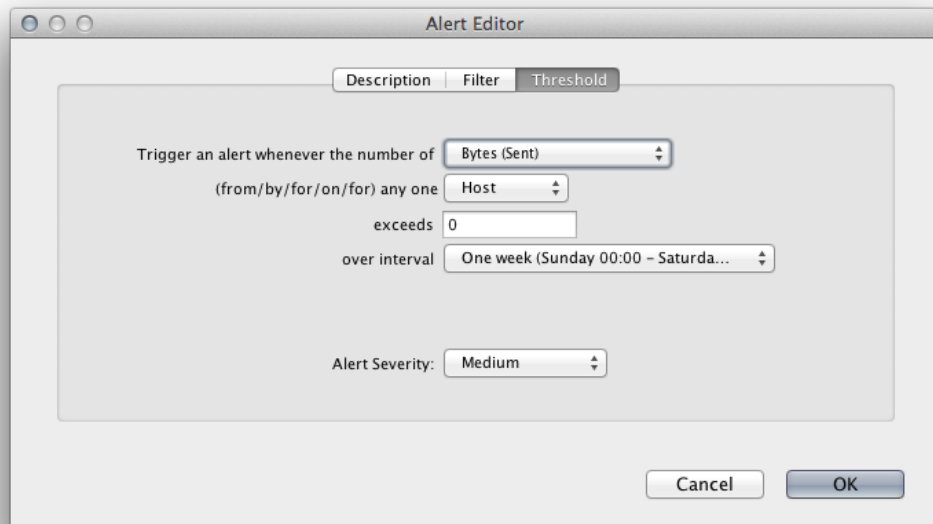
3. On the "Filter" tab, set the session filter you would like to be applied when testing for the alert condition.



i Tip

If you accessed the "Alert Editor" window from a Workspace, the session filter you specified there will be carried over into Alert.

4. On the "Threshold" tab, set the condition on which to generate a notification by using the controls to fill in the blanks of the sentence displayed in the window:



- a. On the first line, select the metric to measure. For instance, you can measure inbound or out-bound bits, bytes, packets, or sessions for each entity.

i Tip

You can also measure the number of *unique* entities an entity associates with. For instance, if you select "unique hosts," FlowTraq will keep track of how many unique hosts are associated with each entity.

- b. On the second line, set the entity on which to measure the the metric. You can choose from Host, Host Pair, Port, or Country.
- c. On the third line, set the threshold, as a numeric value.
- d. On the fourth line, select the time period.
- e. On the final line, select the alert's severity.

i Example

Complete the "Threshold" tab as follows to cause alert to be raised when ever a host contacts more than one hundred unique other hosts in an hour: *Trigger an alert when the number of Unique Hosts for any one Host exceeds 100 over interval One Hour.*

Now go back to the "Filter" tab and set a filter of *Server port is any of: 22* to alert only if a host contacts more than one hundred other unique hosts using the SSH protocol.

5. Click "OK" and the alert will be configured.

Managing and Retrieving Alerts

The Alerts widget provides the interface for retrieving and managing Alerts. To add an Alerts widget to your Dashboard, create it as you would any other widget. (See Chapter 7, *The Dashboard* for more information on managing the Dashboard.)

The Alerts widget has two modes:

- *Show Triggered Alerts*. In this mode, the Alerts widget displays a list of alert notifications; that is, times when an alert condition you set has actually been met.
- *Show Alert Schedule*. In this mode, the Alerts widget displays the list of alerts you have configured.

To toggle between these modes, click the toggle button, which is the first button on the widget's title bar.

Editing, Disabling, and Deleting Alerts

To edit, disable, or delete an alert take the following steps:

1. Put the Alerts widget in *Show Alert Schedule* mode.
2. To edit an alert, double-click on the alert you want to edit, or right-click on it and select "Edit Alert". The "Alert Editor" window will appear. Make the desired changes to the alert's description, filter, or threshold, and click OK to save your changes.

To disable or delete an alert, right-click on the alert you want to disable or delete and select the appropriate item from the context menu.

Viewing Alert Causes

When an alert condition is met, you can view the cause in a workspace. To do so, take the following steps:

1. Place the Alerts widget in *Show Triggered Alerts* mode.
2. Right-click on an alert notification and select from the menu to view one of the following:
 - The earliest time that entity triggered the alert.
 - The most recent time that entity triggered the alert.
 - That entity's entire history with respect to the alert condition.
3. A new workspace window will appear with the timeframe and filter preconfigured to show only the entity which caused the alert condition to be met and the timeframe during which it happened.



Important

If the workspace window is empty, check to see whether there is significant time skew between the computer running FlowTraq Client and the computer running FlowTraq Server. Also, make sure they are both configured to use the same time zone.

Alert Notifications

This section describes how to configure the various alert notification methods.

Notifications on the Dashboard

Alert notifications are automatically displayed on an Alert widget on the Dashboard of the user who set the condition. No action beyond setting the alert condition is necessary to enable alert notifications on the Dashboard.

Tip

You can configure an Alerts widget to display only alert notifications for alerts above a certain severity. Use multiple Alerts widgets to organize your alert notifications in this way.

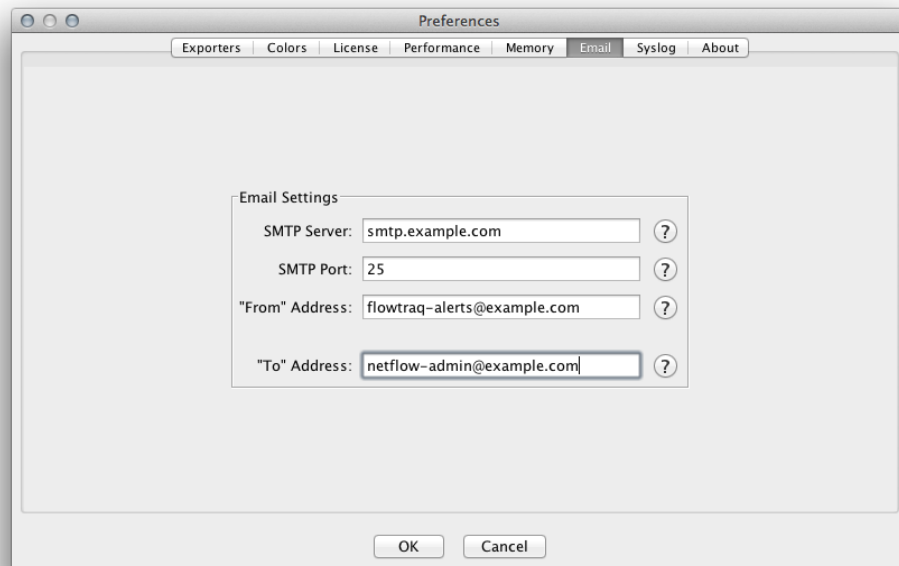
Notifications via E-mail

FlowTraq can send alert notifications via e-mail. FlowTraq uses the SMTP protocol to send alert notification e-mails.

Configuring e-mail alert notification is a two-step process. First, an administrative user must supply FlowTraq with the address (or hostname) and port of an SMTP server, and the e-mail address to use in the "From:" field of all outgoing FlowTraq e-mails. Then, each user who wants to receive e-mail notifications must supply the "To:" address to which they would like their notifications delivered.

To configure e-mail notification for the first time, take the following steps:

1. Log in to FlowTraq as an Administrator.
2. Click the *Preferences* button on the Dashboard window's toolbar, or select *Edit > Preferences* from the menu.
3. Select the *E-mail* tab.



4. Fill in the address (or hostname) of the SMTP server and the port on which it is listening.



Important

FlowTraq does not support SMTP authentication or encryption. Ensure that the SMTP server is configured to allow unauthenticated, unencrypted connections.



Important

The SMTP server must be reachable by FlowTraq Server. Ensure that router and firewall settings allow FlowTraq Server to reach the SMTP server at the configured port.



Tip

Leave this field blank to disable e-mail notifications system-wide.

5. Fill in the desired "From:" address.



"From:" Address

This address will be used for all outgoing FlowTraq e-mails.

6. Fill in the desired "To:" address.



"To:" Address

This address will be used for all alert notifications *for the currently logged-in user* only.



Tip

Leave this field blank to disable e-mail notifications *for the logged-in user*.

7. Click "OK". (A test e-mail will be sent to the "To:" address.)



Important

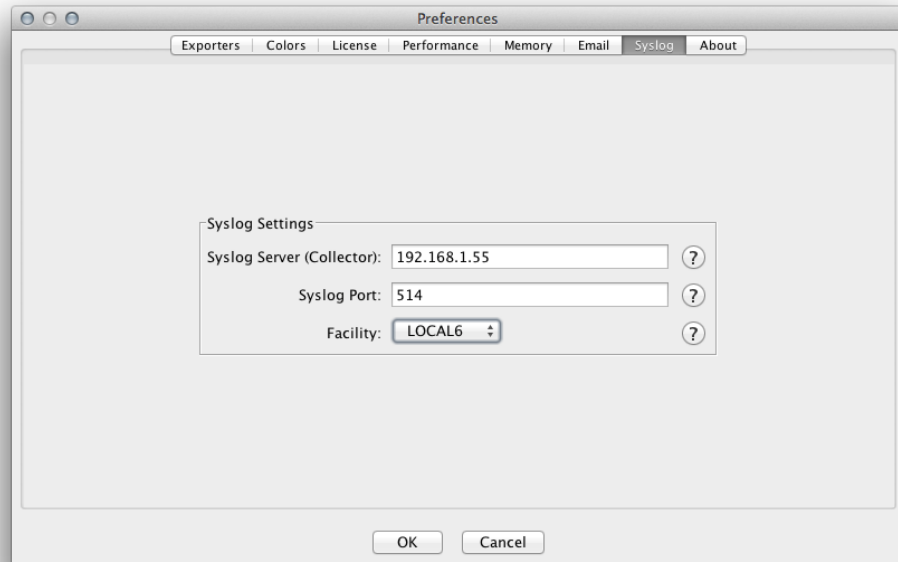
Unprivileged users may access the E-mail preference panel to change the "To:" address for their own alert notifications. However, they may not change the SMTP server, port, or "From:" address.

Notifications via Syslog Over UDP

FlowTraq can send alert notifications via syslog over UDP in order to facilitate integration with third-party SIEM systems.

To configure syslog notifications, take the following steps:

1. Log in to FlowTraq.
2. Click the *Preferences* button on the Dashboard window's toolbar, or select *Edit > Preferences* from the menu.
3. Select the *Syslog* tab.



4. Supply the address (or hostname) of the syslog collector and the port on which it is listening for syslog over UDP. Then select the desired syslog facility.



Important

This configuration be used for all alert notifications *for the currently logged-in user* only.



Important

The syslog collector must be reachable by FlowTraq Server. Ensure that router and firewall settings allow FlowTraq Server to reach the collector at the configured port.



Tip

Leave this field blank to disable syslog notifications *for the currently logged-in user*.

5. Click "OK".

Retrieving Notifications via the Command Line



Important

The command line interface (CLI) is described in detail in Chapter 13, *Command Line Interface*.

FlowTraq notifications can be retrieved via the CLI. This allows you to tie arbitrary scripts to each alert as it is raised. To do this, take the following steps:

1. Using FlowTraq Client, define alerts based on the conditions that you want to act on. (Note: It might make sense to create a dedicated user for scripted alerts.)

2. Retrieve the list of recent alerts by using the `-al`, `-au`, and `-at` parameters with any of the statistical command line tools (e.g. `ns2hostsb`). For example,

```
/opt/flowtraq/cmdline/ns2hostsb -s flowtraq.example.com /  
-un alertuser -up MASKED -al -au alertuser -at -3m
```

This command connects to the FlowTraq Server at `flowtraq.example.com` as user `aler-tuser`. The `-at -3m` requests all the alerts generated for this user in the last 3 minutes.

The output of this command might look something like this:

```
04/11/2012 01:57:03.569706 1 MEDIUM "Upper threshold /  
exceeded on sessions initiated for address /  
xxx.xxx.xxx.xxx." ID=11 type=ANALYTICAL /  
state=NOT-ACKNOWLEDGED user=alertuser /  
v1=17 v2=10  
  
04/11/2012 10:50:03.811054 1 MEDIUM "Upper threshold /  
exceeded on bytes sent for address xxx.xxx.xxx.xxx." /  
ID=13 type=ANALYTICAL state=NOT-ACKNOWLEDGED /  
user=alertuser v1=48 v2=1
```

Legend:

```
MM/DD/YY HH:MM:SS.usec ALERTDEF SEVERITY "MESSAGE" /  
ID=id TYPE=type state=STATE user=USER v1=COUNT /  
v2=THRESHOLD
```

`MM/DD/YY HH:MM:SS.usec` represents the most recent occasion that the referenced ENTITY (host, host pair, country, or port) triggered the alert.

`ALERTDEF` is an integer that uniquely identifies the alert condition.

`SEVERITY` is the severity you selected when you defined the triggered alert, one of `INFO`, `LOW`, `MEDIUM`, `HIGH`, or `CRITICAL`.

`MESSAGE` is a textual representation of the condition which triggered the alert, typically of the form "Upper threshold exceeded on [METRIC] for [ENTITY TYPE] [ENTITY]".

`ID`, `TYPE`, `STATE`, and `USER` can be safely ignored in this context.

`COUNT` is the number of times the referenced ENTITY has caused this alert to trigger. This will be higher if the entity triggers the alert with multiple sessions, or if a triggering session spans multiple alerting periods.

`THRESHOLD` is the threshold you set when you defined the triggered alert.

3. Write a script that consumes the above format, parses out the details you need to guide your action, and takes your desired action. If you are familiar with `/bin/bash`, you might find the following example a helpful starting point:

```
#!/bin/bash

function getAlerts()
{
    /opt/flowtraq/cmdline/ns2hostsb -s flowtraq.example.com /
    -un alertuser -up MASKED -al -au alertuser -at -1m
}

while read line
do
    echo "Processing Alert: " $line
    # add your own code here to parse the details of
    # the alert and take action accordingly
done <<EOF
$(getAlerts)
```

4. Set your script up to run according to a regular schedule (by using `CRON` or similar) as often as you need it to. If your script runs every minute, use `-at 1m` to retrieve the alerts notifications generated in the last minute; if it runs every hour, use `-at 1h`; and so on.

Chapter 12. Server Optimization and Administration

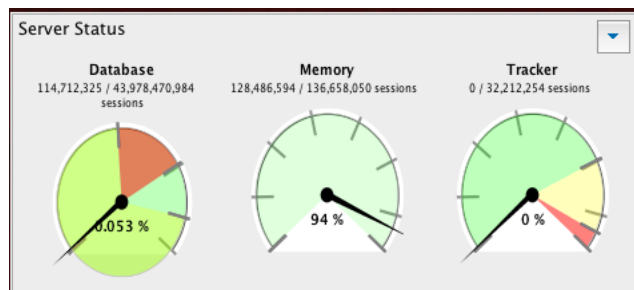
This chapter describes how to configure FlowTraq Server for optimal performance, how to update FlowTraq, and how to perform other routine administrative tasks such as backing up the session database.

Performance Tuning

FlowTraq provides a number of performance indicators to help you determine if FlowTraq is performing well, as well as variety of settings you can adjust to tune performance to your environment.

Performance Indicators

The Server Status Widget



The Server Status Widget provides the following information:

- The number of sessions currently stored in the database.
- The maximum number of sessions which can be stored in the database.
- The number of sessions currently stored in the memory cache.
- The maximum number of sessions which can be stored in the database.
- The number of entries in the connection tracking table.
- The maximum number of entries which can be stored in the connection tracking table.

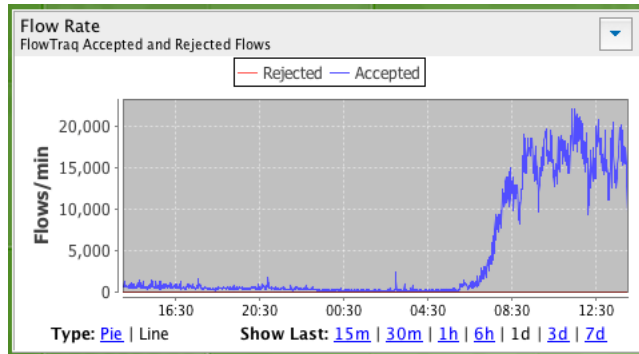
Use these statistics to determine whether to increase the maximum database size or the amount of memory available to FlowTraq. (For information on changing these settings, see the section called “Performance Controls”.)

In particular, watch the database fill statistics to gauge how fast your database is filling at your current flow rate and to help you decide whether to increase your maximum database size or dedicate more storage to FlowTraq. Watch the memory cache statistics to gauge how full your memory cache is. (If interactive queries within a recent timeframe take a long time to perform and your memory cache is full, try increasing the amount of memory available to the cache.) Watch the connection tracker to gauge how well FlowTraq is coping with the incoming flow load.

! Important

When you first install or restart FlowTraq, the memory cache and connection tracking table may take some time to fill.

The Flow Rate Widget



The Flow Rate widget shows the total number of incoming flow updates received by FlowTraq over time as a line graph or a pie chart. It also shows the number of rejected flow updates (FlowTraq Lite licenses only).

! Warning: Flow Rate Statistics Are Not Persistent

If you restart FlowTraq Server (for instance, to upgrade to a newer version or effect a configuration change), the Flow Rate widget will lose its history of rate information. *Flow records are not lost*, but the rate information is. It may take up to a week for the flow rate statistics to re-populate.

! Important: FlowTraq Lite

FlowTraq Lite licenses limit the incoming flow updates to a sustained 100 flows per second. If your network is generally less busy than that, FlowTraq Lite will gracefully handle short bursts above that, but if your flow update rate is persistently over 100 flows per second, it will begin rejecting updates.

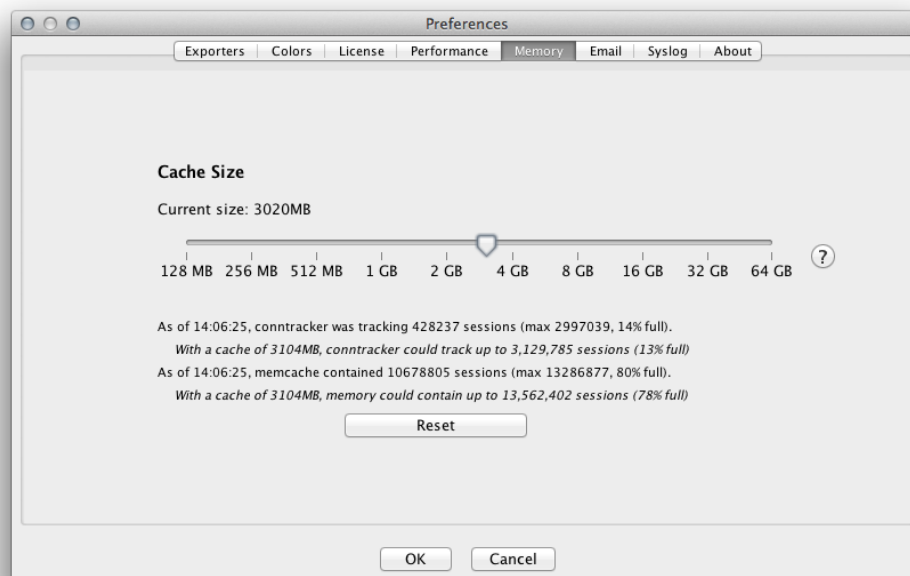
Performance Controls

FlowTraq provides two preference panels, the Memory preference panel and the Performance preference panel, which allow you to adjust various server configuration parameters. They are both accessible from the Dashboard via the *Preferences* toolbar button or the *Edit > Preferences...* menu item.

! Important

The Memory and Performance preference panels are only visible to administrative users.

The Memory Preference Panel



Sessions records are written to disk regularly, but FlowTraq keeps recently-recieved flow updates in memory to allow it to service some queries more quickly. The total amount of memory allocated for the cache is divided between the connection tracker and the memory cache. Please see [sessiontables/conntracksize](#) for more information on the connection tracking engine.

Use the slider on the Memory preference panel to set the size of the connection tracking table and memory cache. The labels below the slider will preview the results of your changes in terms of the number of sessions which can be stored in each part of the cache.

FlowTraq Server Memory Usage

The memory settings you select in the Memory tab in the preferences window is for the session tables only. When setting this value, be sure to leave enough "head room" in physical memory for the operating system, FlowTraq's non-cache memory usage, and for any other processes running on the same machine.

You can calculate the approximate total memory that the FlowTraq server process will use with the following rules.

1. Session tables will grow up to the selected setting in the Memory tab.
2. Each server thread (as configured in the Performance preference panel) will use about 100 megabytes.
3. Each flow listen input port (as configured in the Exporters preference panel) will use 24 megabytes.
4. The database index will use up to about 500 megabytes (for the largest database).
5. Various other server data structures will use about another 200 megabytes.

So, if you select 8 GB in the Memory preference panel on a server with a 16TB database, running 5 flow input ports and 3 server threads, FlowTraq Server itself will use about 9.1 gigabytes of RAM.

Please keep the above in mind when setting the Memory slider. If you do not leave enough head room, or you set this value larger than the system's physical RAM, swap utilization on the machine running FlowTraq Server may increase, causing FlowTraq or the machine to become unresponsive.



Caution: 32-bit environments

On 32-bit platforms, FlowTraq Server will only be able to allocate approximately 2GB of RAM for its memory cache.

Although FlowTraq will work in a 32-bit environment, we strongly recommend that FlowTraq Server be installed on a 64-bit (x86-64) platform.

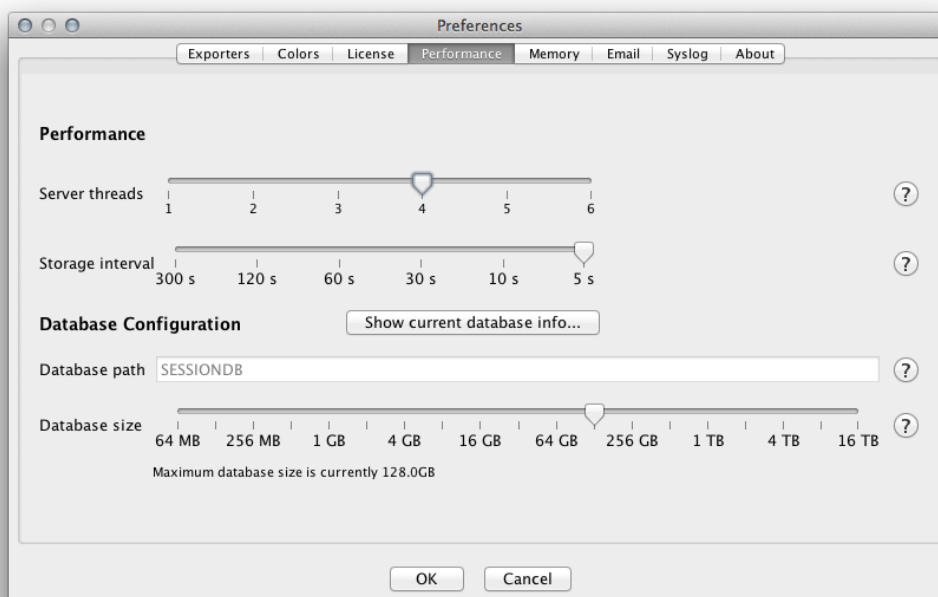
Note that in order to be able to take advantage of a 64-bit platform, both the CPU *and* the operating system must be 64-bit.



Important

Allocating more memory to the cache will increase server startup time, as records are loaded from disk to fill it during startup.

The Performance Preference Panel



The controls on the Performance preference panel can be used to set the number of server threads, the storage interval, and the overall size of the on-disk database, all via sliders.

Please see the definitions of `querythreads` and `storageinterval` in the section called “The FlowTraq Server Configuration File: `flowtraq.conf`” for more information on server threads and the storage interval parameters.

The Session Database

You can resize the maximum size of the session database by using the slider on the Performance preference panel.



Resizing Takes Time

The session database files are not preallocated when you set a maximum size larger than the current maximum size. Likewise, if you set a maximum size smaller than the current database size, the database will be pruned *as new records come in*.

In either case resizing a database is a gradual process. If you change the maximum size of the database here, it will eventually grow or shrink to the new size as new session records arrive.

The location of the session database is displayed in the Performance preference panel, but it cannot be changed while FlowTraq Server is running. Please see the section called “The FlowTraq Server Configuration File: `flowtraq.conf`” for information on changing the location of the session database.

Upgrading FlowTraq

To upgrade FlowTraq, first upgrade FlowTraq Server.

1. Download the installer for latest version of FlowTraq Server allowed by your maintenance agreement to the machine running FlowTraq Server.
2. Run it as though you are installing FlowTraq for the first time (see the section called “Installing or Upgrading FlowTraq Server”).
3. The installer will detect that FlowTraq Server is running, shut it down, upgrade it, and restart it.



Important

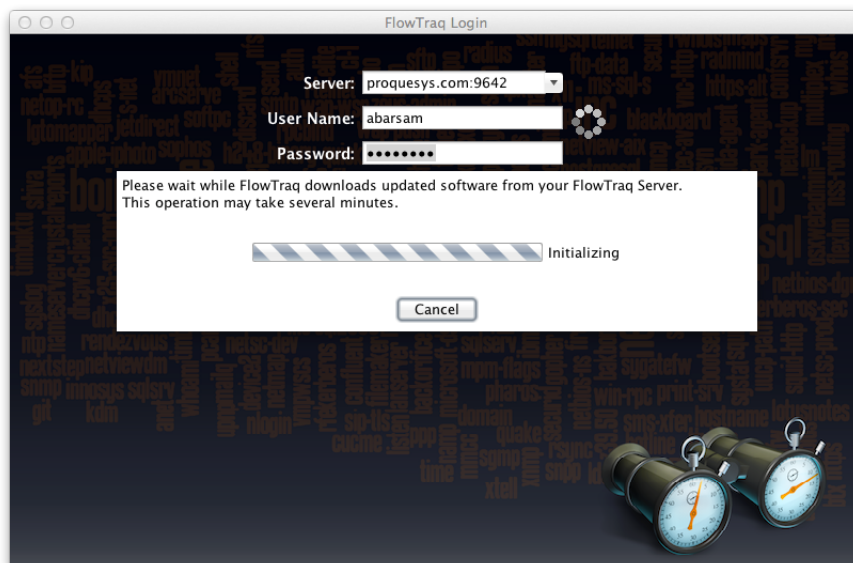
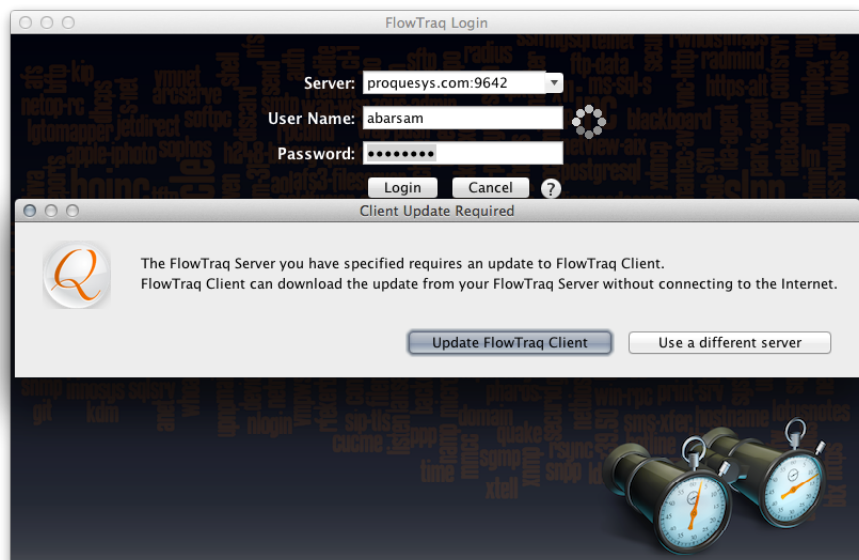
Please note that during the upgrade process, no flow updates will be collected.

Next, upgrade FlowTraq Client, as described below.

Automatic Client Upgrades

FlowTraq requires connecting Clients to be of the same version as the Server to which they are connecting. FlowTraq has the ability to serve Client upgrades from FlowTraq Server without either having to connect to the Internet.

At login time, FlowTraq Server and Client negotiate to determine whether they are of the same version. If they are not, a dialog will appear offering to upgrade or downgrade FlowTraq Client automatically. The process is straightforward.



At the end of the process, FlowTraQ Client will exit. The next time you start FlowTraQ Client, it will be the upgraded version.

There are a few caveats with this process:

1. If either FlowTraQ Client or FlowTraQ Server are older than version Q3/11, they must first be manually updated. Visit the download page, update FlowTraQ Server to the latest version allowed by your maintenance agreement, then do the same for FlowTraQ Client.
2. Note that if you use the same machine to run FlowTraQ Client to connect to two or more instances of FlowTraQ Server of differing versions, you will have to perform this process every time you change which instance you are connecting to. This is because FlowTraQ Client will both upgrade *and* downgrade itself, as needed, to match the remote Server version. To avoid this condition, upgrade all your FlowTraQ Server instances at the same time.

If you experience problems with automatic upgrades, we recommend the following troubleshooting steps.

1. Ensure that FlowTraq Server has been upgraded to the latest version allowed by your maintenance agreement.
2. Uninstall FlowTraq Client on the problematic Client machine.
3. Clear FlowTraq Client's library cache (see the section called "Clearing FlowTraq Client's Library Cache" for more information on this procedure).
4. Reinstall the latest version of FlowTraq Client allowed by your maintenance agreement.

Clearing FlowTraq Client's Library Cache

Issues with FlowTraq Client Automatic Upgrades can sometimes be resolved by clearing FlowTraq Client's library cache.

The library cache can be cleared by deleting the contents of library cache directory (or simply deleting the directory itself). The next time FlowTraq Client is run, it will rebuild the library cache.

The location of the library cache depends on the platform FlowTraq Client is running on.

On Unix platforms (including Mac OS X), the library cache directory is `$HOME/.flowtraq`. To clear it, quit FlowTraq Client, then enter the following at a Terminal:

```
$ rm -rf $HOME/.flowtraq
```

On Windows the library cache directory is `%UserProfile%\flowtraq`. To clear it, quit FlowTraq Client, then enter the following at a command prompt:

```
> cd %UserProfile%\flowtraq  
> del *
```

Advanced Administration

Starting and Stopping FlowTraq Server

The procedure for starting and stopping FlowTraq Server depends on the host operating system.

Windows

On all versions of Windows, use the Services control panel.

1. Click Start, then Run, enter "services.msc" in the Run field, and click Run.
2. In the table that appears, find "ProQueSys FlowTraq Server".
3. Start or stop FlowTraq Server by right-clicking its entry in the table and selecting the appropriate menu item.

Mac OS X

On Mac OS X, use `launchctl`. Open a Terminal window (from Applications->Utilities) and use the following commands to start and stop FlowTraq Server.

```
% sudo launchctl load /  
  /Library/LaunchDaemons/com.proquesys.flowtraq.plist  
% sudo launchctl unload /  
  /Library/LaunchDaemons/com.proquesys.flowtraq.plist
```

Linux

On Linux systems, use the launch script in `/etc/init.d`. Open a shell and use the following commands to start and stop FlowTraq Server.

```
% sudo /etc/init.d/flowtraq start  
% sudo /etc/init.d/flowtraq stop
```

BSD

On BSD, use the launch script in `/etc/rc.d`. Open a shell and use the following commands to start and stop FlowTraq Server.

```
% sudo /etc/rc.d/flowtraq start  
% sudo /etc/rc.d/flowtraq stop
```

Solaris

On Solaris, use `svcadm`. Open a shell and use the following commands to start and stop FlowTraq Server.

```
% sudo svcadm enable flowtraq  
% sudo svcadm disable flowtraq
```

Backing Up the Session Database

It is not necessary to shut down FlowTraq Server in order to back up the session database.

To back up the session database, take the following steps:

1. Copy the full contents of the session database directory to the backup location.



Session Database Location

The default location of the session database depends on the host platform.

On Windows, it is `C:\Program Files\ProQueSys\FlowTraq Server\SESSIONDB`.

On Mac OS X, it is `/Library/Application Support/flowtraq/SESSIONDB`.

On Linux/Solaris/FreeBSD, it is `/opt/flowtraq/SESSIONDB`.

Note that if you edited FlowTraq Server's configuration file or selected a non-default installation directory or session database directory during installation, the session database may be located somewhere else. Check the Performance preference panel of FlowTraq Client.

2. Copy just the index again; that is, re-copy the `ns2xxxxx.metadb` file from the session database directory to the backup location.

Performing the backup in this way helps ensure that the indices are up-to-date. Although it is still theoretically possible to back up an out-of-date index with this technique, the alternative (having to shut the server down for the duration of the backup procedure) would result in significantly more data loss.



Important

If a serious gap in data is found after a recovery, take the following steps.

1. Stop FlowTraq Server. (See the section called “Starting and Stopping FlowTraq Server” for more information on starting and stopping FlowTraq Server.)
2. Delete the index file, `ns2xxxxx.metadb` (located in the session database directory).
3. Start FlowTraq Server.

This will force a re-indexing of the existing data and ensuring data consistency. Note, however, that this operation takes time.

Clearing the FlowTraq Session Database

To clear the FlowTraq session database, take the following steps:

1. Stop FlowTraq Server. (See the section called “Starting and Stopping FlowTraq Server” for more information on starting and stopping FlowTraq Server.)
2. Delete the contents of the session database directory. (Alternatively, move the contents to another folder).
3. Start FlowTraq Server.

Upon restart, the session database directory will be repopulated with files corresponding to an empty database.

The FlowTraq Server Configuration File: `flowtraq.conf`

FlowTraq Server keeps its main configuration parameters stored in a configuration file named `flowtraq.conf`. This file is located in FlowTraq Server's installation directory.



Important

FlowTraq Server may overwrite this file as a result of changes made from FlowTraq Client.

Making Changes to `flowtraq.conf`

The format of `flowtraq.conf` is plain text and is described below. You may edit it using your choice of text editor. However, in order for the changes to take effect, you must either restart FlowTraq

Server (Windows) or signal it (all other operating systems). See the section called “Starting and Stopping FlowTraq Server” for more information on starting and stopping FlowTraq Server.

On non-Windows platforms, signal FlowTraq Server by sending the **SIGHUP** or "hang-up" signal to the **flowtraq** process. To do this, take the following steps:

1. Discover the process ID (PID) of the **flowtraq** process by using the **ps** command:

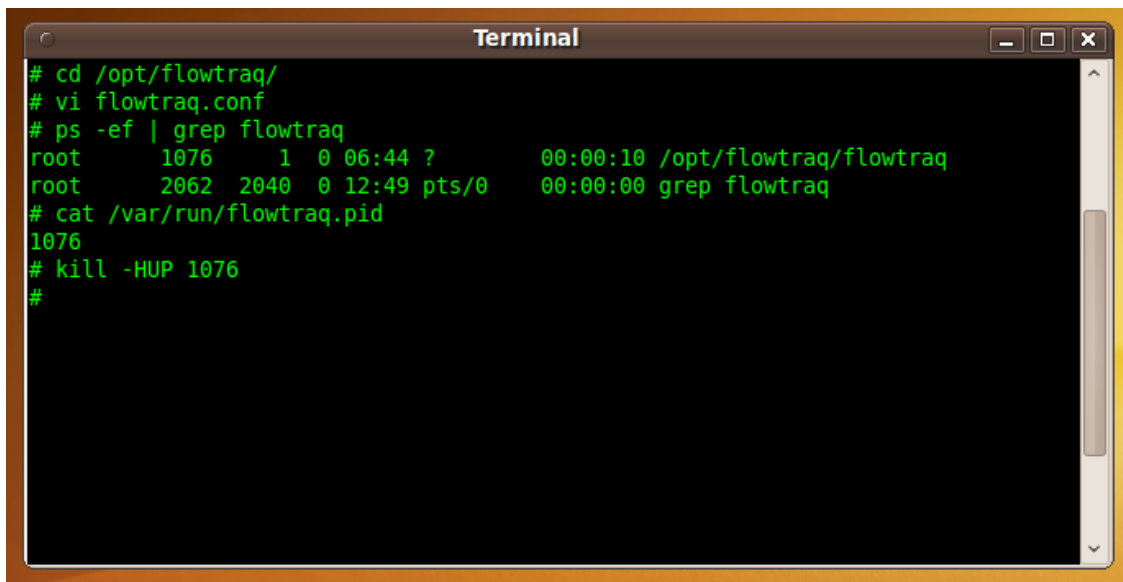
```
% ps -ef | grep flowtraq
```

The PID will be among the output of the **ps** command.

(Alternatively, you may read the contents of the PID file stored in **/var/run/flowtraq.pid**. Note that this technique works on all Unix platforms *except* Mac OS X.)

2. Use **kill** to send the **SIGHUP** signal to **flowtraq**, using the PID you found in step 1:

```
% kill -HUP XXXX
```

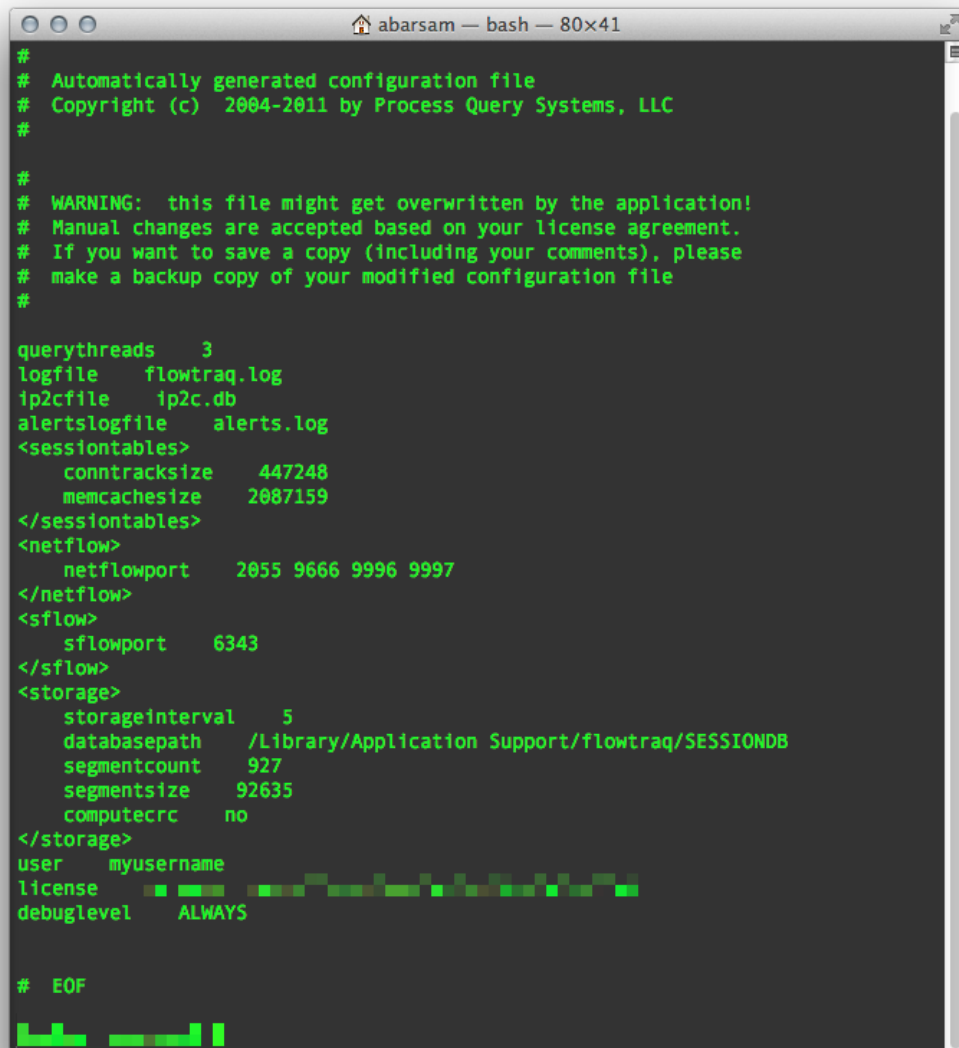
A terminal window titled "Terminal" with a dark background and green text. The window shows a series of commands and their outputs. The commands are: `cd /opt/flowtraq/`, `vi flowtraq.conf`, `ps -ef | grep flowtraq`, `cat /var/run/flowtraq.pid`, and `kill -HUP 1076`. The outputs are: the first two commands have no output, the `ps` command shows two lines of process information, the `cat` command shows the PID 1076, and the `kill` command has no output.

```
# cd /opt/flowtraq/
# vi flowtraq.conf
# ps -ef | grep flowtraq
root      1076      1  0 06:44 ?          00:00:10 /opt/flowtraq/flowtraq
root      2062    2040  0 12:49 pts/0    00:00:00 grep flowtraq
# cat /var/run/flowtraq.pid
1076
# kill -HUP 1076
#
```

Configuration File Format

The FlowTraq configuration file is organized in a key/value-pair hierarchy. In general, configuration keys can appear in any order in the file; however, some related keys must be placed together in sections, which are opened with **<section-name>** tags and closed by **</section-name>** tags.

Below is a typical **flowtraq.conf**.



Notice the sections on `<netflow>`, `<sflow>`, `<sessiontables>`, `<mail>`, and `<storage>`. We will refer to keys in these sessions in their "path" notation: `sflow/sflowport`, indicating that they belong to a specific configuration section.

querythreads

The number of threads the server keeps available to service queries and generate alerts and reports. If there are 4 pending queries, and 3 querythreads, one query will have to wait for a thread to become available before being serviced. Any value between 3 and 6 will usually suffice. We recommend using at least 2 querythreads. The maximum is 20. Each querythread will consume about 100MB of RAM.

ip2cfile

This is the file that FlowTraQ Server uses to resolve IP addresses to country codes. It is a compilation of the IP-to-country files provided by various Internet registries around the world. Each

	version of FlowTraq ships with an updated file. If you would like to receive updates to this file between FlowTraq releases, please contact FlowTraq support.
<code>servicesfile</code>	This is the file that FlowTraq Server uses to resolve server port numbers to application names. It is formatted the same as the common Unix <code>/etc/services</code> file. You can add your own service names to this file.
<code>alertslogfile</code>	This file records all data-driven alerts that are generated by the software. This file will grow over time, and is not automatically rotated.
<code>user</code>	The registered user name associated with the license key. License keys are issued in combination with a username, so it is important to copy your user name accurately.
<code>license</code>	The license key that authorizes FlowTraq. License keys generally look similar to <code>FlowTraq_FULL-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX</code>.
<code>listenport</code>	By default, FlowTraq Server listens on port 9640 for client connections. If you change the listen port number to a privileged port (1024 and below), make sure that FlowTraq Server process runs with administrative privileges.
<code>sessiontables/conntrack-size</code>	Flow data is unidirectional, meaning that the two sides of a conversation are reported independently. For example, if client A requests a webpage from server B, then the flow export data will report separately on the traffic flowing from A to B and from B to A. FlowTraq Server is capable of re-assembling this into a full session record where both sides are put together again. This is done in the connection tracking engine. The number of slots in this engine determines how many concurrent connections can be re-assembled by the FlowTraq Server. A good rule of thumb for determining a sensible value for this key can be computed by counting the number of actively used systems on your network and multiplying that by 400. Another approach is to monitor the number of flows per hour on a busy day, and use the peak number as your value for this key. Each record occupies about 220 bytes of RAM. The value reflects the number of slots allocated, <i>not</i> the amount of memory occupied; multiply by 220 to get the required RAM size. The default value is conservative. Consider increasing this value if RAM is available.
<code>sessiontables/memcache-size</code>	The memory cache in FlowTraq Server caches the most recent flow records in RAM. This allows queries for recent timeframes to run very quickly, as they do not need to retrieve records from the disk database. In general, the larger this cache is, the farther back in time queries can be serviced from RAM without reading from disk. Each record occupies about 160 bytes of memory. Determine your <code>conntracksize</code> first, before allocating RAM to the memory cache, as records are moved through the connection tracking engine to the memory cache. The value reflects the number of slots allocated, <i>not</i> the amount of memory occupied; mul-

	tiply by 160 to get the required RAM size. The default value is conservative. Consider increasing this value if RAM is available.
<code>sessiontables/timeout</code>	By default, records that are in the active conntrack are moved to the memory cache after about 2 hours (7200 seconds). If you set this value to 0, then the records will stay in the connection tracker until it is full. At that point, the connection tracker will move the least recently updated sessions to the memory cache to make room for new incoming flows. Set any other value to change the default timeout. Value is in seconds. The default value is recommended.
<code>sessiontables/toolong</code>	This value controls the breaking up of sessions that are very long-lived into chunks that get stored to disk separately. By default, if a session lasts longer than 8 hours (28800 seconds), then it is split up into multiple records. A flow lasting 24 hours would be stored in 3 session records of 8 hours each. If you don't like this behavior, set this value to 0 to disable it. Breaking very long session up into chunks yields a performance increase when queries are serviced from disk. It has no impact on memory based queries. The default value is recommended.
<code>sessiontables/resizable</code>	The session tables consist of the connection tracking table and the memory cache. By default, these two tables can be resized by storing a different value for their keys to the main configuration file and sending a SIGHUP signal to the FlowTraq Server process. Another way to resize these tables is to move the slider in FlowTraq Client's Memory preferences panel. The ability to resize these tables adds flexibility to FlowTraq's configuration, especially if you are still tuning your parameters. However, a slight performance increase can be realized by fixing the size of these tables to their values given at startup. To fix their sizes, set the value of this key to no.
<code>netflow/netflowport</code>	Typical NetFlow/cFlow/jFlow/IPFIX/NSEL exporters records to UDP/2055, UDP/9666, and/or UDP/9996. FlowTraq Server opens these three ports for collecting incoming datagrams. Each port gets its own input buffer and processing thread. This means that powerful servers under heavy flow load can benefit from opening more ports and configuring exporters to send flows to the alternative ports. Doing this effectively spreads the load and prevents flow packets being dropped. In most scenarios this will be unnecessary. You may enter up to 8 space-separated ports in this list. These ports will handle NetFlow v1/v5/v7/v9, cFlow, jFlow, IPFIX, and NSEL.
<code>netflow/ipfixtcpport</code>	IPFIX exporters can use TCP as the transport protocol. In this case the exporter connects to the FlowTraq server on the given TCP port to transport the IPFIX records. Similar to the UDP NetFlow configuration, opening multiple ports and distributing multiple exporters among them, will spread the CPU load over multiple threads, recuding congestion in busy networks.
<code>netflow/ignoreoldnet-flows</code>	Some NetFlow exporters suffer from heavy time skew. This often happens if the system clocks of the exporters are not properly set.

FlowTraq Server attempts to correct for this. This can be done accurately because the exporters include their sense of the correct time in each NetFlow packet. If the clock of the exporters is set correctly, but the included flow records appear very old, FlowTraq tries to correctly fit them into the history. This may happen, for instance, if you are using old PCAP files as the input source of your flows. By default, this behavior is enabled. If you want to prevent FlowTraq from accepting "old" flow records, then set this value to `no`.

`sflow/sflowport`

By default, FlowTraq Server listens on port UDP/6343 for incoming sFlow packets. Similarly to the `netflowport`, you can enter multiple space-separated port numbers here to make FlowTraq Server listen on different or additional ports for sFlow datagrams. You may enter up to 4 ports in this list. These ports will handle sFlow v2/v4/v5.

`storage/storageinterval`

FlowTraq Server continually tries to store new and updated records in the connection tracking table to the disk database. This is done in a round-robin style. After a pass through the connection tracker, the storage thread will take a brief pause of 5 seconds (by default). This allows systems with heavy I/O load to speed up queries that are serviced from the disk database. Systems under heavy flow load (over 20 million flows per hour) may benefit from setting this parameter to a value as low as 1, while systems with light flow load (up to 4 million flows per hour) can safely set this parameter to values as high as 60. Similarly, if you have very little RAM available, use a lower value, while if you have lots of RAM and a large `conntracksize` value, you can gain disk I/O performance by setting this value higher. In most situations this value does not need tuning.

`storage/databasepath`

This is the location of the disk sessions database. FlowTraq Server will build a hierarchy of files in this directory as flows are received.



Caution

It is not possible to change `storage/databasepath` while FlowTraq Server is running. You must shut down FlowTraq Server before you can change `storage/databasepath`.

`storage/segmentcount`

The `storage/segmentcount` key sets the number of disk segments the on-disk session database is divided into.

This key, together with `storage/segmentsize` (the number of session records stored in each disk segment), determines the overall size of the session database. Each session record occupies about 200 bytes, so the number of bytes that the database will use is approximately `segmentcount x segmentsize x 200`.

FlowTraq uses a custom sequential database with time-based indexing. Records are grouped in segments of a fixed number of records. Each segment corresponds to a file on disk, and the num-

ber of segments in this database can have a substantial influence on the duration that disk-based queries will take.

Modern filesystems support directories with thousands of files in them, and FlowTraq can take advantage of many files, so it is safe to set the `segmentcount` in the thousands.



Tip

If you set the database size via FlowTraq Client's Performance preference panel, `storage/segmentcount` and `storage/segmentsize` are set according to a formula.



Tip

Resizing a database is a gradual process. If you change the maximum size of the database, it will eventually grow or shrink to the new size as new session records arrive.

`storage/segmentsize`

The `storage/segmentsize` key sets the number of session records stored in each disk segment.

This key, together with `storage/segmentcount`, determines the overall size of the session database. Please see the description for `storage/segmentcount` for more information on this key.

`userdata/userdatapath`

FlowTraq stores all user settings, reports, and workspace files in a separate directory. By default this directory is named `USERDATA` and is created in FlowTraq Server's installation directory. By setting `userdatapath`, the location of these files can be changed.



Caution

It is not possible to change `storage/userdatapath` while FlowTraq Server is running. You must shut down the FlowTraq server before you can change `storage/userdatapath`.

`userdata/maxsession-keyage`

The commandline tools included with FlowTraq can establish a persistent session with the FlowTraq server based on pre-authenticated session keys. These keys can be generated with the `'-us'` option to any commandline tool, and subsequently used to re-authenticate from the same IP address for a short amount of time. The time-out of session keys can be configured with the `'userdata/maxsessionkeyage'` in the server configuration file. The default timeout (in seconds) is 0, disabling the session key functionality. Set to a positive number to enable.

`mail/server`

The hostname or IP address of the SMTP server that FlowTraq should use to send e-mail notifications of user-configurable alerts.

`mail/port`

The port of the SMTP server that FlowTraq should use to send e-mail notifications of user-configurable alerts (usually 25).

<code>mail/from</code>	The e-mail address from which the alert notifications should appear to be sent from.
<code>debuglevel</code>	This determines how verbose FlowTraq should be when writing to <code>logfile</code> . In ascending order of verbosity, this key may be set to one of the following values: ALWAYS, CRITICAL, HIGH, MEDIUM, LOW. Be careful when using the more verbose settings such as LOW, as the log file may grow to be very large over time.
<code>maxclientlatency</code>	This is the number of seconds that FlowTraq will wait for a client to acknowledge a session download before disconnecting the client. Raw session record downloads (with the GUI, or 'ns2sq') can consume a large amount of network resources, causing other clients to slow down. If a client does not respond to the FlowTraq server in the specified amount of time, the raw session download is cancelled. The default value is 60 seconds. Lower values are recommended for busier system. Set to 0 to disable this feature.

Chapter 13. Command Line Interface

The FlowTraq Command Line Interface (CLI) provides an easy way for custom scripts and third party applications to query FlowTraq Server for flow information.

The CLI tools are installed with FlowTraq Server in the `/path/to/flowtraq/clitools` directory.

Tip

The CLI tools, like the client, connect to FlowTraq Server via 9640/tcp. You don't have to run the CLI tools from the host on which you installed FlowTraq Server.

Overview

There are three CLI tools.

<code>ftsq</code>	<i>FlowTraq Session Query Retrieval Tool.</i> The <code>ftsq</code> command allows you to retrieve bi-directional session data assembled from the unidirectional flow data. This command accepts as parameters a report type, a timeframe, and an optional filter string to narrow the scope of the report. It presents its results as CSV or a pretty-printed ASCII table.
<code>ftstat</code>	<i>FlowTraq Statistical Query Retrieval Tool.</i> Use <code>ftstat</code> to retrieve the kinds of statistical reports you can retrieve in a FlowTraq Workspace, such as "Hosts Ranked by Bytes Sent" or "Applications ranked by Sessions Received". Like the <code>ftsq</code> command, <code>ftstat</code> accepts a timeframe and filter string. It presents tabular results as either CSV or a pretty-printed ASCII table, while graphical results are written to disk in the TARGA graphics file format (TGA).
<code>ftum</code>	<i>FlowTraq User Management.</i> The <code>ftum</code> command allows you to create and delete users, reset passwords, and grant administrative privileges.

Retrieving Raw Session Data from the Command Line with `ftsq`

To retrieve raw session records, use the `ftsq` command.

For example, the following invocation of `ftsq` returns all records in the last hour to HTTP servers with a client address that is outside the 123.45.67.89 class-C block, in CSV format with a header line:

Figure 13.1. `ftsq` Example

```

eagle:clitools abarsam$ ./ftsq -s webdev -un admin -up admin -tn -lh -c+ -q "SRVPORT==80 && CLNIP!=123.45.67.89/24"
CLIENT ADDRESS, CLIENT COUNTRY, CLIENT AS, SPORT, SERVER ADDRESS, SERVER COUNTRY, SERVER AS, DPORT, PROTO, CLN PKTS,
CLN BYTES, SRV PKTS, SRV BYTES, START TIME, LAST UPDATE, TTIME, FLAGS, TOS, EXPORTER ADDRESS, IFIN, IFOUT, VLANIN, VL
ANDUT, CLNMAC, SRVMAC
87.252.82.194, NO, 0, 45982, 216.107.218.226, US, 0, 80, TCP, 5, 272, 3, 172, 10/12/2012 13:03:52.016000, 10/12/2012
13:04:03.870000, 11.854, ...AP.SF, 0x00, 192.168.68.1, 0016, 001c, 0, 0, 00:23:33:80:84:c0, e0:91:f5:21:cf:7e
87.252.82.194, NO, 0, 41207, 216.107.218.226, US, 0, 80, TCP, 21, 9384, 13, 2371, 10/12/2012 12:48:04.702000, 10/12/2
012 12:48:46.981000, 42.199, ...AP.SF, 0x00, 192.168.68.1, 0016, 001c, 0, 0, 00:23:33:80:84:c0, e0:91:f5:21:cf:7e
216.107.218.226, US, 0, 58626, 173.194.73.103, US, 0, 80, TCP, 7, 2551, 5, 1540, 10/12/2012 12:46:49.982000, 10/12/20
12 12:47:49.874000, 59.892, ...AP.SF, 0x00, 192.168.68.1, 001c, 0014, 0, 0, e0:91:f5:21:cf:7e, 00:23:33:80:84:c0
87.252.82.194, NO, 0, 33375, 216.107.218.226, US, 0, 80, TCP, 43, 17705, 37, 27184, 10/12/2012 12:48:04.701000, 10/12
/2012 12:48:46.981000, 42.2, ...AP.SF, 0x00, 192.168.68.1, 0016, 001c, 0, 0, 00:23:33:80:84:c0, e0:91:f5:21:cf:7e
87.252.82.194, NO, 0, 37698, 216.107.218.226, US, 0, 80, TCP, 40, 20168, 22, 5586, 10/12/2012 13:02:12.025000, 10/12/
2012 13:02:53.754000, 41.729, ...AP.SF, 0x00, 192.168.68.1, 0016, 001c, 0, 0, 00:23:33:80:84:c0, e0:91:f5:21:cf:7e
216.107.218.226, US, 0, 58620, 173.194.75.105, US, 0, 80, TCP, 7, 2551, 5, 1540, 10/12/2012 12:41:49.737000, 10/12/20
12 12:42:49.161000, 59.424, ...AP.SF, 0x00, 192.168.68.1, 001c, 0014, 0, 0, e0:91:f5:21:cf:7e, 00:23:33:80:84:c0
216.107.218.226, US, 0, 58719, 173.194.75.99, US, 0, 80, TCP, 10, 5129, 7, 1151, 10/12/2012 13:24:10.983000, 10/12/20
12 13:25:10.982000, 59.999, ...AP.SF, 0x00, 192.168.68.1, 001c, 000e, 0, 0, e0:91:f5:21:cf:7e, 00:23:33:80:84:c0
87.252.82.194, NO, 0, 40432, 216.107.218.226, US, 0, 80, TCP, 37, 10202, 21, 4464, 10/12/2012 13:02:12.024000, 10/12/
2012 13:02:53.754000, 41.73, ...AP.SF, 0x00, 192.168.68.1, 0016, 001c, 0, 0, 00:23:33:80:84:c0, e0:91:f5:21:cf:7e
87.252.82.194, NO, 0, 34336, 216.107.218.226, US, 0, 80, TCP, 41, 14014, 47, 46989, 10/12/2012 12:46:21.498000, 10/12
/2012 12:47:06.973000, 45.475, ...AP.SF, 0x00, 192.168.68.1, 0016, 001c, 0, 0, 00:23:33:80:84:c0, e0:91:f5:21:cf:7e
216.107.218.226, US, 0, 58612, 173.194.75.99, US, 0, 80, TCP, 7, 2551, 5, 1540, 10/12/2012 12:36:49.124000, 10/12/201
2 12:37:45.475000, 56.351, ...AP.SF, 0x00, 192.168.68.1, 001c, 000e, 0, 0, e0:91:f5:21:cf:7e, 00:23:33:80:84:c0
216.107.218.226, US, 0, 2396, 69.59.227.139, US, 0, 80, TCP, 5, 438, 4, 1348, 10/12/2012 13:04:39.699000, 10/12/2012
13:04:39.749000, 0.05, ...AP.SF, 0x00, 192.168.68.1, 001c, 001f, 0, 0, e0:91:f5:21:cf:7e, 00:23:33:80:84:c0
87.252.82.194, NO, 0, 47503, 216.107.218.226, US, 0, 80, TCP, 11, 1781, 13, 13118, 10/12/2012 12:55:46.907000, 10/12/
2012 12:56:03.717000, 16.73, ...AP.SF, 0x00, 192.168.68.1, 0016, 001c, 0, 0, 00:23:33:80:84:c0, e0:91:f5:21:cf:7e
87.252.82.194, NO, 0, 48951, 216.107.218.226, US, 0, 80, TCP, 12, 4760, 0, 1539, 10/12/2012 12:46:21.353000, 10/12/20
12 12:46:36.968000, 15.615, ...AP.SF, 0x00, 192.168.68.1, 0016, 001c, 0, 0, 00:23:33:80:84:c0, e0:91:f5:21:cf:7e
216.107.218.226, US, 0, 58710, 173.194.75.147, US, 0, 80, TCP, 6, 2499, 5, 2402, 10/12/2012 13:22:39.913000, 10/12/20
12 13:23:39.908000, 59.995, ...AP.SF, 0x00, 192.168.68.1, 001c, 001e, 0, 0, e0:91:f5:21:cf:7e, 00:23:33:80:84:c0
87.252.82.194, NO, 0, 36585, 216.107.218.226, US, 0, 80, TCP, 22, 0696, 19, 13222, 10/12/2012 12:47:39.140000, 10/12/

```

The `ftsq` commands accepts a wide range of parameters. Some are optional and some are required.

You should always specify a FlowTraq Server to log in to (or accept the default, `localhost`), supply a username and password, and select a timeframe over which to perform your query (or accept the default, which is the last 15 minutes).

Optionally, you may supply a filter string to further narrow your query, and you may specify a preference for how you would like the command's output formatted.

Most of the parameters are self-explanatory, but timeframe specification and the filter string syntax are described in depth in the section called “Time Navigation” and the section called “Filter String Syntax”. First, however, please review the complete list of parameters:

Table 13.1. Connection Parameters

Parameter	Description
-s SERVER	Address (or hostname) of FlowTraq server to query. (Default: <code>localhost</code> .)
-p PORT	Port on which to connect to FlowTraq server. (Default: 9640.)

Table 13.2. Login Parameters

Parameter	Description
-un USER	Username for profile login. <i>Required</i> .
-up PASS	Password for profile login. (Note: If you do not use <code>-up</code> , you will be prompted to enter a password.)

Parameter	Description
-us [SESSIONKEY]	Authenticate with a session key rather than with a username and password, or generate a session key. (For more information, see the section called “Session Key Reauthentication”).

Table 13.3. Timeframe Parameters

Parameter	Description
-te "MM/DD/YY hh:mm:ss.microsec"	Specify an absolute timeframe starting time. Must be used in conjunction with -tl . Cannot be used in conjunction with -tn .
-tl "MM/DD/YY hh:mm:ss.microsec"	Specify an absolute timeframe ending time. Must be used in conjunction with -te . Cannot be used in conjunction with -tn .
-tn RELTIME	Specify a timeframe relative to now (e.g. -tn -1h30m for the last 1.5 hours). Default: last 15 minutes. Cannot be used in conjunction with -te or -ts. Please see the section called “Time Navigation” for more information on valid specifiers for RELTIME.

Table 13.4. Filtering Parameters

Parameter	Description
-e IP	Filter for flows from exporter with a given IP address. Default: all exporters. Must be specified before -ei and -ef .
-ei INDEX	Filter for flows with a given interface index of exporter. Default: all interfaces.
-ef [nf1 nf5 nf9 sf2 sf4 sf5]	Filter for flows from a given exporter version. Default: any version.
-snd	The -snd parameter indicates that FlowTraq should only count outbound packets, bytes, or sessions when generating rankings. May not be used in conjunction with the -rcv parameter.
-rcv	The -rcv parameter indicates that FlowTraq should only count inbound packets, bytes, or sessions when generating rankings. May not be used in conjunction with the -snd parameter.
-q "RAWQUERY"	Specify a query string (enclose in ""-pair). See the section called “Filter String Syntax” for a description of the query string syntax.

**Important**

Note that the -snd and -rcv parameters are not applicable to the `ftsquery` command, since rankings are not generated when returning raw session records. Use these parameters in conjunction with `ftstat`, as described below.

Table 13.5. Output Parameters

Parameter	Description
<code>-w NUM</code>	Create a time series with <code>NUM</code> slices. Default: don't create a time series.
<code>-r num</code>	Number of rows per table. Default: 128.
<code>-c</code>	Use CSV output format.
<code>-c+</code>	Use CSV output format with headers and summaries.
<code>-v</code>	Display a progress indicator. Useful for longer summary queries.
<code>-g filename.tga</code>	If specified, in addition to writing the tabular result to the terminal, the command will write a stack chart to <code>filename.tga</code> . Default: don't write a stack graph.
<code>-gx X</code>	The width, in pixels, of the image produced. May only be used in conjunction with <code>-g</code> and <code>-gy</code> .
<code>-gy Y</code>	The height, in pixels, of the image produced. May only be used in conjunction with <code>-g</code> and <code>-gx</code> .

**Important**

Note that the `-w` parameter is not applicable to the `ftsquery` command, since there is no accompanying time series for raw session records. Use this parameter in conjunction with `ftstat`, as described below.

**Important**

Note that the `-g`, `-gx`, and `-gy` parameters are not applicable to the `ftsquery` command, since there is no accompanying stack graph for raw session records. Use these parameters in conjunction with `ftstat`, as described below.

Time Navigation

Both `ftstat` and `ftsquery` require a timeframe specification.

You can set an absolute timeframe by specifying start and end times with `-te` and `-tl`. Specify both a starting and ending time in the following format: "`MM/DD/YY hh:mm:ss.microsec`".

Alternatively, you can specify a timeframe relative to now by using the `-tn` option. For example, `-tn -1h` specifies the last hour, `-tn -1d12h` specifies the day and a half, and `-tn -5m` specifies the last five minutes.

Valid time specifiers for the `-tn` option are as follows:

<code>s</code>	Seconds
<code>m</code>	Minutes
<code>h</code>	Hours

d	Days
w	Weeks
M	Months
y	Years



Important

Time specifiers must be given in order of magnitude. This means that `-tn -2d1w` is an invalid way to specify "the last 9 days". Instead, use `-tn -1w2d`, which is valid.

Filter String Syntax

All data retrieval commands accept an optional filter string. The filter string is used to select which sessions to include in the retrieval.

Filter strings consist of statements, such as `SRVIP==123.45.67.89` ("server IP address is 123.45.67.89") and `CLNPKTS>=100` ("number of client-transmitted packets is at least 100"), which may be combined using logical operators.

You can combine statements using the following logical operators:

<code>&&</code>	logical 'AND'
<code> </code>	logical 'OR'
<code>^ </code>	logical 'XOR' (exclusive-OR)
<code>!</code>	logical 'NOT'

For example: `SRVIP==123.45.67.89 && CLNIP==89.67.45.123 .`



Tip

You can build compound statements and specify precedence by using parentheses. For example, you might use:

```
(SRVPORT==22 && SRVIP==123.45.67.89) || (SRVIP==89.67.45.123)
```

to specify all sessions which are either connections on port 22 to 123.45.67.89, or connections on ANY port to 89.67.45.123.

Statements are formed by combining field names (such as `SRVIP`) with comparators (such as `==`) and values to compare them to. The following lists the available comparators and field names.

Comparators

<code>==</code>	equals
<code>!=</code>	does not equal
<code>>=</code>	greater than or equal to
<code><=</code>	less than or equal to

> greater than
< less than

Table 13.6. Filter String Fields

Field	Description	Valid Comparators
SRVIP	server IP (or CIDR), IPv4: 123.45.67.89/32, or IPv6: fed9::c0:ffee/128	==, !=
CLNIP	client IP (or CIDR), same as SRVIP	==, !=
ADDR	IP or CIDR block	==, !=
SRVPORT	server port, integer number	==, !=, >=, <=, >, <
CLNPORT	client port, integer number	==, !=, >=, <=, >, <
PORT	port, integer number	==, !=, >=, <=, >, <
PROTO	protocol, one of TCP/UDP/ ICMP, or integer number	==, !=, >=, <=, >, <
CLNPKTS	number of client transmitted packets, integer number	==, !=, >=, <=, >, <
SRVPKTS	number of server transmitted packets, integer number	==, !=, >=, <=, >, <
PACKETS	match either of the packet fields (server or client), integer num- ber	==, !=, >=, <=, >, <
TOTPKTS	total packets (server plus client), integer number	==, !=, >=, <=, >, <
CLNBYTES	number of client transmitted bytes, integer number	==, !=, >=, <=, >, <
SRVBYS	number of server transmitted bytes, integer number	==, !=, >=, <=, >, <
BYTES	match either of the bytes fields (server or client), integer num- ber	==, !=, >=, <=, >, <
TOTBYTES	total bytes (server plus client), integer number	==, !=, >=, <=, >, <
TTIME	total time of session, floating point, in seconds: 2.5	==, !=, >=, <=, >, <
TOS	ToS, QoS, DiffServ, integer number 0-256	==, !=, >=, <=, >, <
CLNCC	client country code, two charac- ters: 'US', 'NL'	==, !=
SRVCC	server country code, same as client country code	==, !=
INIF	inbound interface, integer num- ber 0-65536	==, !=, >=, <=, >, <

Field	Description	Valid Comparators
OUTIF	outbound interface, integer number 0-65536	==, !=, >=, <=, >, <
IFACE	match either of the interface fields (inbound or outbound), integer number 0-65536	==, !=, >=, <=, >, <
INVLAN	inbound VLAN, integer number 0-4096	==, !=, >=, <=, >, <
OUTVLAN	outbound VLAN, integer number 0-4096	==, !=, >=, <=, >, <
VLAN	match either of the VLAN fields (inbound or outbound), integer number 0-4096	==, !=, >=, <=, >, <
CLNAS	client autonomous system number, integer number	==, !=, >=, <=, >, <
SRVAS	server autonomous system number, integer number	==, !=, >=, <=, >, <
ASN	match either of the autonomous system number fields (server or client), integer number	==, !=, >=, <=, >, <
ASAEVT	ASA event code, integer number	==, !=, >=, <=, >, <
ASAEVTEVT	ASA extended event code, integer number	==, !=, >=, <=, >, <
FLAGS	TCP flags in session, one of: 'FSYN' (syn), 'FACK' (ack), 'FRST' (reset), 'FFIN' (fin), 'FPSH' (push), 'FECN' (ECN-echo), 'FCWR' (congestion window reduced), 'FURG' (urgent)	==, !=
EXPIP	IP of the device that exported the record	==, !=
EXPV	flow version, use: 1, 5, 7, 9 (NetFlow v1/5/7/9), 18, 20, 21 (sFlow v2/4/5)	==, !=

Retrieving Statistical Queries from the Command Line with `ftstat`

The FlowTraq Statistical Query Retrieval command `ftstat` creates tables and graphs of grouped items that are ranked by some criterion. For example, you can retrieve the list of hosts that *sent* the most packets during a given timeframe or the list of hosts that *received* the most packets during the same. You can also find out which *port/application* accounted for the most bytes on your network, find which *host pair* exchanged the most bytes, and more.

It is also possible to score by more complex criteria. For instance, it is possible to find the list of *hosts* that contacted the *largest number of unique hosts*, or the list of *countries* that contacted your servers on the *largest number of unique server ports*.

As with the `ftsquery` command, you must specify a FlowTraq Server to connect to, supply login details, select a timeframe and (optionally) specify a filter. And like `ftsquery`, the results are returned in a formatted table, by default, or in CSV format (use either the `-c` option for CSV without a header, or the `-c +` option for CSV with a header line). Please refer to the complete list of parameters in the section called “Retrieving Raw Session Data from the Command Line with `ftsquery`” [109], the section called “Filter String Syntax” for more information on the filter language syntax, and the section called “Time Navigation” for information on timeframe specifications.

Where the usage of `ftstat` differs from that of `ftsquery` is in specifying the desired statistic to calculate. Specify the statistic by using the `-grp` and `-cnt` parameters:

Table 13.7. Statistical Query Parameters

Parameter	Description
<code>-grp ENTITY_TYPE</code>	Create a ranking of the given entity type, one of: IP, IPPAIR, PORTPROTO, QOS, TCPFLAGS, IF, IFPAIR, COUNTRY, VLAN, VLANPAIR, ASN, ASNPAIR, MAC, or MACPAIR.
<code>-cnt COUNT</code>	Rank entities on the specified field, one of: BYTES, BITS, SESSIONS, PACKETS, or UNIQUE. UNIQUE requires an additional argument, one of: IP, PORTPROTO, QOS, TCPFLAGS, IF, COUNTRY, VLAN, ASN, or MAC

ftstat Example 1

To retrieve the top 25 hosts by bytes sent in the last week, use the following command:

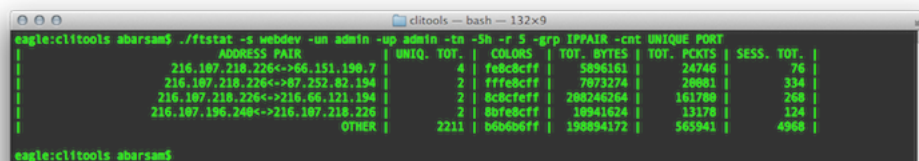
```

eagle:clitools abarsam$ ./ftstat -s webdev -un admin -up admin -tn -lw -r 25 -grp HOST -cnt BYTES -snd
| ADDRESS | SENT BYTES | COLORS | SENT BYTES | RECV BYTES | SENT PKTS | RECV PKTS | SESS. INIT | SESS. ACPT |
| 216.187.218.226 | 8285796316 | fe8c8c7f | 8285796316 | 9122282541 | 12824435 | 11232287 | 78529 | 14386 |
| 72.21.211.199 | 1882918883 | f7fe8c7f | 1882918883 | 19487237 | 668775 | 455423 | 0 | 28 |
| 207.171.163.225 | 932668881 | 8c8c7f | 932668881 | 17672412 | 621939 | 414868 | 0 | 9 |
| 216.66.121.194 | 757261357 | 8bfe8c7f | 757261357 | 51858888 | 632469 | 86364 | 2633 | 0 |
| 207.171.163.131 | 566887241 | 8cfe8c7f | 566887241 | 11142787 | 377543 | 268538 | 0 | 5 |
| 205.251.242.196 | 475371768 | fe8c7f | 475371768 | 8971622 | 316974 | 212145 | 0 | 9 |
| 205.251.242.38 | 473132958 | b48b8c7f | 473132958 | 8884285 | 315451 | 287145 | 0 | 3 |
| 205.251.242.132 | 394415171 | b3b8c7f | 394415171 | 7648838 | 263883 | 379488 | 0 | 6 |
| 72.21.215.164 | 328386187 | 8c8b5ff | 328386187 | 6162117 | 218919 | 146641 | 0 | 0 |
| 207.171.163.161 | 269919929 | 8c8b5ff | 269919929 | 4928692 | 188889 | 117822 | 0 | 13 |
| 173.194.31.178 | 214358518 | 8ab3b5ff | 214358518 | 2996873 | 143311 | 78528 | 0 | 10 |
| 72.21.214.143 | 187388728 | b58ab3ff | 187388728 | 3688938 | 124966 | 84921 | 0 | 3 |
| 207.171.163.3 | 151995582 | f88c8c7f | 151995582 | 2788872 | 181334 | 64821 | 0 | 1 |
| 216.187.196.241 | 121174778 | f8f88c7f | 121174778 | 3778538 | 85333 | 47273 | 0 | 679 |
| 72.21.194.15 | 188198966 | 898c7fff | 188198966 | 1933943 | 66948 | 44658 | 0 | 9 |
| 65.96.7.188 | 88398338 | 8cfc8c7f | 88398338 | 6988858488 | 1523253 | 4754169 | 0 | 340 |
| 12.230.288.134 | 84618879 | 8c7ff7c7f | 84618879 | 54451317 | 633315 | 393749 | 0 | 23 |
| 64.48.185.183 | 82678885 | fcb87fff | 82678885 | 24248597 | 183878 | 212485 | 0 | 12758 |
| 72.21.211.178 | 77135624 | b3888c7f | 77135624 | 1459586 | 51463 | 34591 | 0 | 10 |
| 208.88.186.186 | 76787837 | b2b58c7f | 76787837 | 3556296 | 87161 | 67488 | 0 | 1 |
| 66.151.198.7 | 73919719 | 89898c7f | 73919719 | 29821899 | 157812 | 227132 | 96 | 954 |
| 173.194.31.166 | 71273898 | 88b58c7f | 71273898 | 1133119 | 47535 | 21285 | 0 | 4 |
| 66.151.198.6 | 69789393 | 8c8b5ff | 69789393 | 6318588 | 59658 | 48589 | 2 | 1960 |
| 216.187.196.233 | 65518681 | b58c8c7f | 65518681 | 2797628 | 47268 | 24311 | 0 | 644 |
| OTHER | 2456987437 | b6b68c7f | 2456987437 | 1822953588 | 4345446 | 4658274 | 11655 | 61852 |

```

ftstat Example 2

To retrieve the five host-pairs that communicated over the largest number of ports during last five hours, use the following command:



```
eagle:clitools abarsam$ ./ftstat -s webdev -un admin -up admin -tn -sh -r 5 -grp IPPAIR -cnt UNIQUE PORT
ADDRESS PAIR      UNIQ. TOT.  COLORS  TOT. BYTES  TOT. PKTS  SESS. TOT.
|-----|
| 216.107.210.226<->66.151.190.7 |      4 | f08c8cfff | 5896161 | 24746 | 76 |
| 216.107.210.226<->87.252.82.194 |      2 | fffe8cfff | 7073274 | 20001 | 334 |
| 216.107.210.226<->216.06.121.194 |      2 | 8c8cfefff | 200246204 | 161700 | 260 |
| 216.107.190.240<->216.107.210.226 |      2 | 8bf8cfff | 10941624 | 13178 | 124 |
| OTHER |      2211 | 60b0bfff | 190094172 | 565941 | 4900 |
eagle:clitools abarsam$
```

Tip

You may use the `-g` parameter to request the accompanying stack graph, and the `-gx` and `-gy` parameters to specify the size of the graph you would like.

Tip

You may use the `-w` parameter to request a timeseries for each row of the table.

Managing Users from the Command Line with **ftum**

To manage users, use the `ftum` command.

You must specify a FlowTraq Server to connect to and supply login details.

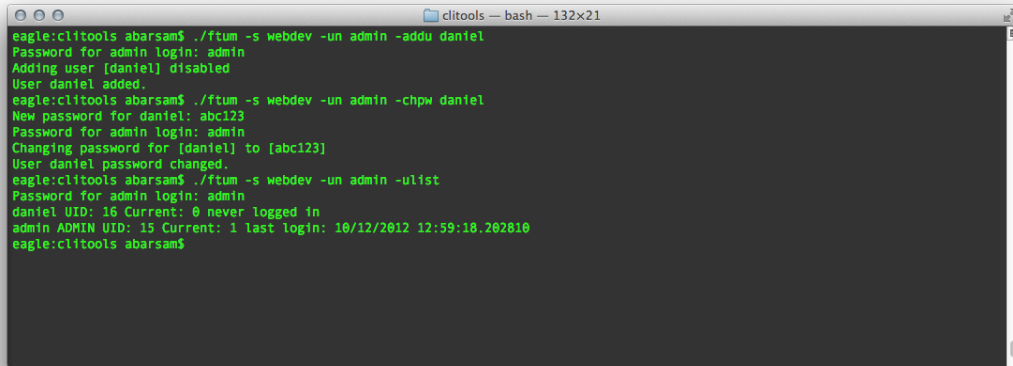
In addition to the connection and login parameters, `ftum` accepts the following parameters:

Table 13.8. User Management Parameters

Parameter	Description
<code>-chpw USERNAME PASSWORD</code>	Change password for user <code>USERNAME</code> to <code>PASSWORD</code> . You must log in as <code>USERNAME</code> to perform this action for yourself, or as an administrator to perform this action for an arbitrary user.
<code>-addu USERNAME PASSWORD</code>	Add a new user, <code>USERNAME</code> , with initial password <code>PASSWORD</code> . You must log in as an administrator to perform this action.
<code>-delu USERNAME</code>	Delete user <code>USERNAME</code> . You must log in as an administrator to perform this action.
<code>-admin USERNAME</code>	Grant administrative privileges to user <code>USERNAME</code> . You must log in as an administrator to perform this action.
<code>-noadmin</code>	Revoke administrative privileges from user <code>USERNAME</code> . You must log in as an administrator to perform this action.

Parameter	Description
<code>-ulist</code>	Print the list of users. You must log in as an administrator to perform this action.

For example, to add a new user (with the `-addu` option) and set the initial password (with the `-chpw` option), take the following steps:



```
eagle:clitools abarsam$ ./ftum -s webdev -un admin -addu daniel
Password for admin login: admin
Adding user [daniel] disabled
User daniel added.
eagle:clitools abarsam$ ./ftum -s webdev -un admin -chpw daniel
New password for daniel: abc123
Password for admin login: admin
Changing password for [daniel] to [abc123]
User daniel password changed.
eagle:clitools abarsam$ ./ftum -s webdev -un admin -ulist
Password for admin login: admin
daniel UID: 16 Current: 0 never logged in
admin ADMIN UID: 15 Current: 1 last login: 10/12/2012 12:59:18.202810
eagle:clitools abarsam$
```

Session Key Reauthentication

The session key reauthentication mechanism allows for FlowTraq's command line tools to be easily integrated with third-party applications and applications hosted on other systems. The use of session keys allows automated scripts and script-based interfaces such as web GUIs to call additional command line tools without the need to store the username and password in a client-side cookie. Since the session key automatically expires, and is only valid from the originating IP address, it is unnecessary to perform an explicit "log out."



Disabled by Default

FlowTraq Server is not configured by default to use session keys. In order to enable session keys, the configuration file `flowtraq.conf` needs to be modified, and the FlowTraq service restarted. The following example allows for session keys to timeout after 120 seconds.

```
<userdata>
  maxsessionkeyage 120
  [...]
</userdata>
```

Please see the section called "Configuration File Format" for more information on configuring session key reauthentication.

To create and use a session key, a command line tool must first provide a valid user's credentials to log into a session, and provide the `-us` parameter to request that a session key be created. Any command will work, but `ftum` is convenient because it doesn't need to interact with session data, so we use it in our example:

```
ftum -un USERNAME -up PASSWORD -us
```

If the credentials provided are valid, the `stderr` output of the command will be a session key; for example:

```
91389bd1127bce0a2615d390be08f696
```

The session key may subsequently be used with the `-us` argument instead of a username/password combination to re-login to the same FlowTraq Server from the same IP address. Continuing our example:

```
ftstat -us 91389bd1127bce0a2615d390be08f696 [...]
```



Tip

Each time the session key is used, the timer is reset. The session key will eventually expire on the server side after the period of time specified in the `userdata/maxsessionkeyage` configuration parameter.

Retrieving Alert Notifications via the Command Line

Please see the section called “Retrieving Notifications via the Command Line” for more information on retrieving alert notifications via the CLI.

Chapter 14. The FlowTraq Network Behavioral Intelligence Toolkit

In addition to FlowTraq Client and the command line interface, FlowTraq offers a suite of network behavioral anomaly detection tools, which are referred to as the Network Behavioral Intelligence Toolkit.

The Toolkit consists of a number of configurable, purpose-built detectors that connect to a FlowTraq Server, detect certain kinds of behaviors, and log detected behaviors to syslog. In this respect, they are similar to the threshold-based Alerts that can be set via the Client. However, the Toolkit's detectors are not threshold-based; rather, each detector uses intelligent machine learning algorithms to pinpoint which traffic sessions on the network are unusual, interesting, or potentially malicious. The tools in the Toolkit study your traffic and generate a behavioral fingerprint of your network, which they then use to decide if communications are potentially anomalous.

Overview

The tools in the toolkit are implemented as command-line tools that function as stand-alone processes. When run, they first establish a connection to a FlowTraq Server, examine the Server's forensic history to establish baselines, and then begin detecting and logging behaviors.

The CLI tools are installed with FlowTraq Server in the `/path/to/flowtraq/nbitools` directory. You don't have to run the CLI tools from the host on which you installed FlowTraq Server.

Below is an overview of the detectors in the Toolkit.

<code>ftbfg</code>	The FlowTraq Behavioral Fingerprint Generator alerts on connections which it finds "unusual" based on baseline behavior observed during a learning period. Generally a training period is specified (last month, last year, ...), and optionally a filter (monitor outbound, 1 specific server, all non-HTTP, etc). FTBFG quickly uses historical data to train, and applies smart behavioral algorithms to recognize related subnets, typical relationships, and external CDNs.
<code>ftdos</code>	The FlowTraq Denial-of-Service detector alerts on unusually high levels of incoming connections from one or more sources. As such, it can be used to detect both DDoS attempts as well as brute-force attacks such as password-guessing or "fuzzing". This detector can be configured to monitor a range of addresses and destination ports or simply to monitor all inbound traffic.
<code>ftscan</code>	The FlowTraq Scan detector detects both vertical (port) and horizontal (host) scans. Any host connecting to an unusually high number of ports, or an unusually high number of other hosts, is logged. Threats such as worm propagation, advanced persistent threats, and cyber reconnaissance are detected with <code>ftscan</code> , as can spam relays.
<code>fttcv</code>	The FlowTraq Typical Connection Volume detector alerts on substantial changes in connection volume (either inbound or outbound) for any IP address in the monitored range. Time-of-day and time-of-week information is included in the behavioral signa-

ture to recognize periodic patterns intelligently. This detector can also pick up on new hosts in your network, hosts that disappear, and DNS amplification attacks.

Configuration

Basic Parameters

The FlowTraq NBI Tools share a number of basic configuration parameters in common with the CLI tools; in particular, the `-s`, `-p`, `-un`, `-up`, `-us`, `-q`, `-e`, `-ei`, and `-ef` parameters all work in the same way as they do with the CLI tools. Use these to specify the FlowTraq Server to connect to, the credentials to use to log in, and more. For more information on these parameters, please see the section called “Retrieving Raw Session Data from the Command Line with `ftsqr`” [109].

NBI Tools and FlowTraq Filters

You can even use `-q`, `-e`, `-ei`, and `-ef` with standard FlowTraq filters to control what traffic is examined. This allows for very fine grained control over the alerts that are generated, strongly reducing false positives.

Training Options

The FlowTraq NBI Tools all learn network behavioral baselines by first examining a period of historical data. When they are run, they first perform a learning pass over a specified timeframe of historical data (the “training period”), compute baselines, and then begin alerting in real time on the live traffic as it arrives. Specify the training period by using the `-tn` parameter (to specify a training period relative to now) or using `-te/-tl` to specify an absolute training period. For more information on these parameters, please see the section called “Retrieving Raw Session Data from the Command Line with `ftsqr`” [109].

Logging Options

All of the NBI tools support logging network behavior anomalies to standard out or to syslog. To configure logging, use the following parameters.

Table 14.1. Logging Parameters

Parameter	Description
<code>-ls</code>	Log to stdout (Default: yes UNLESS a loghost is specified via <code>-lh</code>)
<code>-lh LOGHOST</code>	Loghost, specify where syslog message are to be sent (Default: syslog is disabled)
<code>-lp PORT</code>	Syslog port on the loghost (Default: 512)
<code>-lf FACILITY</code>	yslog facility, one of: LOCAL0-LOCAL7. (Default: LOCAL0)
<code>-ll LEVEL</code>	Syslog level, one of: EMERG, ALERT, CRIT, ERR, WARNING, NOTICE, INFO, DEBUG. (Default: NOTICE)
<code>-lu MESSAGE</code>	User-defined custom message to be added at the end of the syslog message. Enclose in ""-pair.

Usage Notes

It is often advisable to run multiple instances of one or more of the NBI tools to control alerting channels, priorities, and load balance. You can use `-lf`, `-ll`, and `-lu` to tell instances apart at the log collector. To get the full benefit of the NBI tools, run at least one of each tool.

ftbfg

The FlowTraq Behavioral Fingerprint Generator requires very little configuration. Besides the basic options and the learning period, there is only one parameter to specify.

Table 14.2. ftbfg-specific Parameters

Parameter	Description
<code>-bc N</code>	Behavioral fingerprint complexity index (default: 1, max: 16)

A higher complexity index generates a better fingerprint, but takes longer to generate. Here is an example of `ftbfg` output:

```
host:nbitools user$ ./ftbfg -s SERVER -un USER -up PASS -tn 4w
Learning...
Progress: | 100.000% 15943 records [....]
Optimizing behavioral fingerprint... Complexity 7.81

10/15/2012 16:14:39.870553 unusual connection
from 1.2.3.4 to 4.3.2.1 443/TCP

10/15/2012 16:14:37.707855 unusual connection
from 2.3.4.5 to 5.4.3.2 123/UDP

10/15/2012 16:14:36.366546 unusual connection
from 3.4.5.6 to 6.5.4.3 53/UDP

10/15/2012 16:14:40.350553 unusual connection
from 4.5.6.7 to 7.6.5.4 443/TCP

10/15/2012 16:14:36.365546 unusual connection
from 5.6.7.8 to 8.7.6.5 53/UDP

[...]
```

ftdos

The FlowTraq DOS Detector requires a few configuration parameters besides the basic options and the learning period. They are:

Table 14.3. ftdos-specific Parameters

Parameter	Description
-bg	Behavioral granularity, one of: WEEK (hourly slices), DAY (10 minute slices). Default: DAY.
-bt	Absolute threshold. Don't alert unless values are above threshold (default: 100)



Important

When using -bg WEEK, the detector runs every 10 minutes, requesting an hour.

When using -bg DAY, the detector runs every 2 minutes, requesting 10 minutes.

DAY may have up to a 120 second lag between start of attack and the detection, while WEEK has up to a 600 second lag. However, WEEK puts a smaller load on the system than DAY.

If DDOS mitigation is a priority, you must run the DOS detector in DAY mode. However, other detectors that do not require immediate automated response may be more accurate in WEEK mode.



Exclude Local Addresses

Consider using a filter to exclude your local CIDR block from the DOS detector if you use automatic mitigation. Or be a good Internet neighbor and block local addresses that are originating too many connections.

Here is an example of ftdos output:

```
host:nbitools user$ ./ftdos -s SERVER -un USER -up PASS
Learning...
Estimated iterations: 1.01042
Progress: / 100.000% 1737392 records [....]
Training complete, tracking 4094 entities...

10/15/2012 16:31:04.446711 DOS behavior detected from
source 1.2.3.4 to target 4.3.2.1 during 10/15/2012
16:20:00 to 10/15/2012 16:30:00: 273 connections initiated

10/15/2012 16:31:04.446749 DOS behavior detected from
source 2.3.4.5 to target 5.4.3.2 during 10/15/2012
16:20:00 to 10/15/2012 16:30:00: 148 connections initiated

10/15/2012 16:31:04.446760 DOS behavior detected from
source 3.4.5.6 to target 6.5.4.3 during 10/15/2012
16:20:00 to 10/15/2012 16:30:00: 101 connections initiated

[...]
```

ftscan

The FlowTraq Scan Detector tool accepts the `-bg/-bt` parameters. Their interpretation, use, and caveats, is the same as in `ftdos`. Please see the section called “`ftdos`” for more information on these.

Here is an example of `ftscan` output:

```
host:nbitools user$ ./ftscan -s SERVER -un USER -up PASS
Learning...
Estimated iterations: 1.00149
Progress: - 100.000% 1931638 records [....]
Training complete, tracking 254 entities...

10/15/2012 16:32:23.992240 host/horizontal SCAN detected
from source 1.2.3.4 during 10/15/2012 15:30:00 to 10/15/2012
16:30:00: 1370 unique hosts scanned

10/15/2012 16:32:23.992289 host/horizontal SCAN detected
from source 2.3.4.5 during 10/15/2012 15:30:00 to 10/15/2012
16:30:00: 275 unique hosts scanned

10/15/2012 16:32:23.992306 host/horizontal SCAN detected
from source 3.4.5.6 during 10/15/2012 15:30:00 to 10/15/2012
16:30:00: 221 unique hosts scanned

[...]
```

fttcv

The FlowTraq Typical Connection Volume tool is the most configurable tool in the NBI toolkit. Like `ftscan` and `ftdos`, `fttcv` accepts the basic parameters, the training period parameters, and the `-bg/-bt` parameters. Please see the section called “`ftdos`” and the section called “`ftbfg`” for more information on these.

However, `fttcv` also accepts a parameter to specify how many standard deviations away from baseline a measurement must be to alert on. Measurements can be significantly higher OR lower than baseline to trigger an alert:

Table 14.4. `fttcv`-specific Parameters

Parameter	Description
<code>-bk</code>	Anomaly threshold: number of standard deviations away from mean (default: 3) to trigger alert.

Futhermore, `fttcv` accepts the `-grp/-cnt/-snd/-rcv` parameters to specify exactly what to measure about what entities. Astute readers may notice that the `ftdos` and `ftscan` commands can be approximated with judicious use of these parameters with `fttcv`.

Here is an example of `fttcv` output:

```
host:nbitools user$ ./fttcv -s SERVER -un USER -up PASS -grp  
HOST -cnt BYTES
```

Learning...

Estimated iterations: 9

Progress: \ 100.000% 1612679 records [d...]

Progress: \ 100.000% 4183841 records [d...]

Progress: / 100.000% 5135777 records [d...]

Progress: / 100.000% 7033539 records [d...]

Progress: | 100.000% 6527109 records [....]

Progress: \ 100.000% 0 records [....]

Progress: - 100.000% 0 records [....]

Progress: / 100.000% 3674372 records [....]

Progress: / 100.000% 1928253 records [....]

Training complete, tracking 12636 entities...

10/15/2012 16:50:51.749012 unusually HIGH volume for total bytes
communicated by address 1.2.3.4 during 10/15/2012 15:50:00
to 10/15/2012 16:50:00: 1110337644.00
(u: 1110337644.00 s: 0.00 k: -1.00 n: 1)

10/15/2012 16:50:51.749193 unusually HIGH volume for total bytes
communicated by address 2.3.4.5 during 10/15/2012 15:50:00
to 10/15/2012 16:50:00: 944856533.00
(u: 152723952.99 s: 331763734.18 k: 11.55 n: 7)

10/15/2012 16:50:51.749456 unusually HIGH volume for total bytes
communicated by address 3.4.5.6 during 10/15/2012 15:50:00
to 10/15/2012 16:50:00: 938749314.00
(u: 167720982.61 s: 352670922.12 k: 11.41 n: 6)

[...]

Appendix A. Enabling Flow Export on Common Devices

This appendix contains quick-start guides for enabling flow export on common devices. Please consult your network device's documentation for more information.

CISCO IOS

This is a quick-start guide for enabling NetFlow export on CISCO IOS version 12.4.

1. Begin by logging into your switch or router using `telnet`.
2. Enter the privileged EXEC mode (password required) using the `enable` command.

```
# enable
```
3. Enter the global configuration mode using the `configure terminal` command.

```
# configure terminal
```
4. At this point, configure a flow monitor on all the interfaces that you want to monitor using the `ip route-cache flow` command for each. (In our example below, we configure a flow monitor on the FastEthernet0/0 and FastEthernet0/1 interfaces).

```
# interface FastEthernet0/0
# ip route-cache flow
# exit
# interface FastEthernet0/1
# ip route-cache flow
# exit
```

5. Once the interfaces have been configured to collect NetFlow statistics, you will need to configure the export destination. In the configuration terminal, set the destination:

```
# ip flow-export destination 192.168.17.3 2055
```

This sets the export destination to host 192.168.17.3, port UDP/2055. Of course, you will want to replace 192.168.17.3 with the address of the host running FlowTraq Server.

6. Select the source of the flow information:

```
# ip flow-export source FastEthernet0/0
```

7. Set the preferred NetFlow version, one of 1, 5, 7, or 9:

```
#ip flow-export version 5
```



Important

You must use NetFlow version 9 if you have IPv6 traffic on your network.

8. Configure the export policy for active connections:

```
# ip flow-cache timeout active 1
```

This command configures the exporting of active connections once per minute. This means that the flow statistics of, e.g., a streaming video are exported to the FlowTraQ collector every 60 seconds even if more packets are expected later in the session.

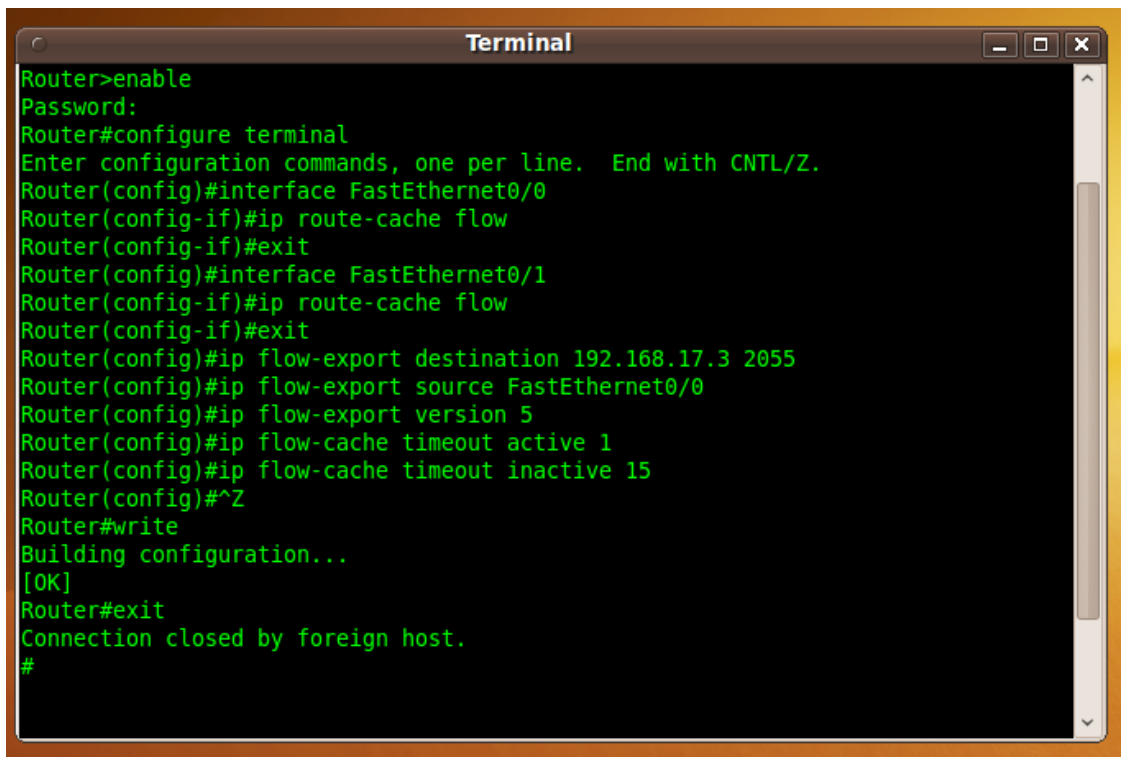
9. Configure the export policy for connections that have been closed or have become inactive:

```
# ip flow-cache timeout inactive 15
```

This command tells the NetFlow exporting engine that sessions that have seen no new packets for more than 15 seconds should be exported at that time. A lower value here reduces the load on your CISCO device CPU, but increases NetFlow export traffic on your network. A value of 15 is commonly used as a good compromise.

10. Exit the configuration terminal with CTRL-Z.

11. Store the new configuration by using the `write` command before closing the connection.



```
Router>enable
Password:
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ip route-cache flow
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip route-cache flow
Router(config-if)#exit
Router(config)#ip flow-export destination 192.168.17.3 2055
Router(config)#ip flow-export source FastEthernet0/0
Router(config)#ip flow-export version 5
Router(config)#ip flow-cache timeout active 1
Router(config)#ip flow-cache timeout inactive 15
Router(config)#^Z
Router#write
Building configuration...
[OK]
Router#exit
Connection closed by foreign host.
#
```

Appendix B. FlowProxy

This chapter describes FlowTraq FlowProxy. FlowProxy is a flow forwarder which listens for flow updates on one or more ports, then reformats the flows into IPFIX, tags them with a unique custom identifier, and forwards them to a specified FlowTraq Server destination.

You can use FlowProxy's tagging capability to distinguish flows from an exporter or group of exporters (e.g. to keep customer data apart on a shared FlowTraq instance).

FlowProxy is a part of the FlowTraq suite.

Installing FlowProxy

At this time, FlowProxy is only supported on the following platforms:

Table B.1. FlowProxy Platform Support

Platform	Architecture	Startup Method
Debian Linux, Ubuntu Linux, and variants	32-bit Intel (x86), 64-bit Intel (x86-64)	Using <code>/etc/init.d</code> and <code>/etc/rc*</code>
RedHat Linux, CentOS, and variants	32-bit Intel (x86), 64-bit Intel (x86-64)	Using the <code>chkconfig</code> system
SUSE Linux, OpenSUSE and variants	32-bit Intel (x86), 64-bit Intel (x86-64)	Using <code>/etc/sbin/rc*</code>
Solaris	64-bit SPARC, 64-bit Intel (x86-64)	Using SVC manifests
FreeBSD	32-bit, 64-bit Intel (x86-64)	Using <code>/etc/rc.d</code>
Mac OS X	64-bit Intel (x86-64)	Using <code>launchd</code>



FlowTraq and FlowProxy on the Same Machine

We do not recommend you run both FlowTraq and FlowProxy on the same machine; if you do, however, you may be required to manually reconfigure FlowTraq to avoid undesired behavior.



GUID tagging

The FlowProxy installer will ask you to provide a GUID to use. All traffic forwarded by this proxy will be tagged with the GUID. If you need a GUID, please contact FlowTraq support: support@flowtraq.com

To install FlowProxy, take the following steps.

1. Download the universal Unix installer (`FlowProxy-QX_XX-PLATFORM.sh.gz`, where `QX_XX` represents the current version of FlowProxy).
2. Unzip the installer:

```
$ gunzip FlowProxy-QX_XX-PLATFORM.sh.gz
```

This produces `FlowProxy-QX_XX-PLATFORM.sh`.

3. Run the installer with superuser privileges, either by running as root or via `sudo`:

```
$ sudo sh FlowProxy-QX_XX-PLATFORM.sh
```

4. Press [SPACE] to page through the license agreement, and type YES when prompted to indicate your acceptance.
5. If this is a new installation, you will be asked to select the installation directory. You can press [ENTER] to accept the default installation directory, or you can specify your own.



Important

The permissions on the installation directory must allow the `flowproxy` process to write to the directory, as it will update various items at runtime.

If you are upgrading an existing FlowProxy installation, the current configuration is retained and the new proxy daemon is started right away. Otherwise, follow the prompts to provide FlowProxy with the information it needs to produce its initial configuration.

FlowProxy will start automatically once installation is complete, and will be set to start automatically upon startup.

Starting and Stopping FlowTraq Server

The procedure for starting and stopping FlowTraq Server depends on the host operating system.

Windows

On all versions of Windows, use the Services control panel.

1. Click Start, then Run, enter "services.msc" in the Run field, and click Run.
2. In the table that appears, find "ProQueSys FlowTraq Server".
3. Start or stop FlowTraq Server by right-clicking its entry in the table and selecting the appropriate menu item.

Mac OS X

On Mac OS X, use `launchctl`. Open a Terminal window (from Applications->Utilities) and use the following commands to start and stop FlowTraq Server.

```
% sudo launchctl load /  
/Library/LaunchDaemons/com.proquesys.flowtraq.plist  
% sudo launchctl unload /  
/Library/LaunchDaemons/com.proquesys.flowtraq.plist
```

Linux

On Linux systems, use the launch script in `/etc/init.d`. Open a shell and use the following commands to start and stop FlowTraq Server.

```
% sudo /etc/init.d/flowtraq start
% sudo /etc/init.d/flowtraq stop
```

BSD

On BSD, use the launch script in `/etc/rc.d`. Open a shell and use the following commands to start and stop FlowTraq Server.

```
% sudo /etc/rc.d/flowtraq start
% sudo /etc/rc.d/flowtraq stop
```

Solaris

On Solaris, use `svcadm`. Open a shell and use the following commands to start and stop FlowTraq Server.

```
% sudo svcadm enable flowtraq
% sudo svcadm disable flowtraq
```

The FlowProxy Configuration File

FlowProxy keeps its main configuration parameters stored in a configuration file named `flowproxy.conf`. This file is located in FlowProxy's installation directory.

Making Changes to `flowproxy.conf`

The format of `flowproxy.conf` is plain text and is described below. You may edit it using your choice of text editor. However, in order for the changes to take effect, you must signal it to reload.

Signal FlowProxy to reload by sending the `SIGHUP` or "hang-up" signal to the `flowproxy` process. To do this, take the following steps:

1. Discover the process ID (PID) of the `flowproxy` process by using the `ps` command:

```
% ps -ef | grep flowproxy
```

The PID will be among the output of the `ps` command.

(Alternatively, you may read the contents of the PID file stored in `/var/run/flowproxy.pid`. Note that this technique works on all Unix platforms *except* Mac OS X.)

2. Use `kill` to send the `SIGHUP` signal to `flowproxy`, using the PID you found in step 1:

```
% kill -HUP XXXX
```

Configuration File Format

The FlowProxy configuration file is organized in a key/value-pair hierarchy. In general, configuration keys can appear in any order in the file; however, some related keys must be placed together in sections, which are opened with `<section-name>` tags and closed by `</section-name>` tags.

<code>netflow/netflowport</code>	Typical NetFlow/cFlow/jFlow/IPFIX/NSEL exporters records to UDP/2055, UDP/9666, and/or UDP/9996. FlowProxy opens these three ports for collecting incoming datagrams. Each port gets its own input buffer and processing thread. This means that powerful servers under heavy flow load can benefit from opening more ports and configuring exporters to send flows to the alternative ports. Doing this effectively spreads the load and prevents flow packets being dropped. In most scenarios this will be unnecessary. You may enter up to 8 space-separated ports in this list. These ports will handle NetFlow v1/v5/v7/v9, cFlow, jFlow, IPFIX, and NSEL.
<code>netflow/ipfixtcpport</code>	IPFIX exporters can use TCP as the transport protocol. In this case the exporter connects to the FlowProxy on the given TCP port to transport the IPFIX records. Similar to the UDP NetFlow configuration, opening multiple ports and distributing multiple exporters among them, will spread the CPU load over multiple threads, recuding congestion in busy networks.
<code>sflow/sflowport</code>	By default, FlowProxy listens on port UDP/6343 for incoming sFlow packets. Similarly to the <code>netflowport</code> , you can enter multiple space-separated port numbers here to make FlowTraq Server listen on different or additional ports for sFlow datagrams. You may enter up to 4 ports in this list. These ports will handle sFlow v2/v4/v5.
<code>debuglevel</code>	This determines how verbose FlowTraq should be when writing to <code>logfile</code> . In ascending order of verbosity, this key may be set to one of the following values: ALWAYS, CRITICAL, HIGH, MEDIUM, LOW. Be careful when using the more verbose settings such as LOW, as the log file may grow to be very large over time.
<code>recursion/guid</code> XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	All traffic forwarded by this proxy will be tagged with this GUID. If you need a GUID, please contact FlowTraq support: support@flowtraq.com Note: GUIDs have the form: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
<code>recursion/forwarder0</code> IP PORT	All traffic forwarded by this proxy will be sent to the destination IP and port (IPFIX over TCP) specified here

Appendix C. FlowTraq Web API Reference

The FlowTraq Web API provides a RESTful interface for for retrieving NetFlow data from a FlowTraq Server in JSON format for use by third-party applications. This API defines two methods of retrieving data:

1. NetFlow data processed into specific FlowTraq views
2. Raw NetFlow session records as stored by FlowTraq

Authentication

An API authentication token is required for all requests. Authentication tokens must be generated for each client through the FlowTraq command line tools. To request the token, send an HTTP request such as:

POST `https://example.com/flowtraq/api/v1/auth`

Request Parameters

Parameter Name	Value	Default Value	Notes
server	string	"localhost"	The FlowTraq server address.
port	number	9640	The FlowTraq server port.
username	string	<i>required</i>	Username of a user on the Flowtraq server.
password	string	<i>required</i>	Password of the Flow- traq server user.

Response Parameters

The response will contain either the resulting auth token or an error message:

Parameter Name	Value	Notes
auth_token	string	Only returned if authentication successful.
error	string	Only returned if authentication failed.

Example

For example, using curl in a shell command:

```
$ curl -d "https://example.com/flowtraq/api/v1/auth" -d "username=admin&password=admin"
```

```
{"auth_token": "6334b9326ec3268bfb6dc801d831c829"}
```

Retrieving Processed FlowTraq Views

Various FlowTraq view combinations may be retrieved via the API by sending requests to:

GET <https://example.com/flowtraq/api/v1/stat>

Request Parameters

Parameter Name	Value	Default Value	Notes
server	string	"localhost"	The FlowTraq server address.
port	number	9640	The FlowTraq server port.
auth_token	string	<i>required</i>	A recently acquired authentication token from an authentication request.
group_by	string	"IP"	A rank entity as described in Retrieving Statistical Queries from the Command Line [http://support.flowtraq.com/Documentation/Q4_12/webhelp/content/ch11s05.html].
count_by	string	"BYTES"	A rank field as described in Retrieving Statistical Queries from the Command Line [http://support.flowtraq.com/Documentation/Q4_12/webhelp/content/ch11s05.html]. Use a space to separate the token "unique".
direction	string	<i>none</i>	Possible values: "snd", "rcv".
before_time	timestamp	<i>none</i>	A timestamp in the format "MM/DD/YY hh:mm:ss.microsec".
after_time	timestamp	<i>none</i>	A timestamp in the format "MM/DD/YY hh:mm:ss.microsec".

Parameter Name	Value	Default Value	Notes
time_range	string	-15m	A time specifier as described in Time Navigation [http://support.flowtraq.com/Documentation/Q4_12/webhelp/content/retime.html].
query	string	<i>none</i>	A filter string as described in Filter String Syntax [http://support.flowtraq.com/Documentation/Q4_12/webhelp/content/filterlanguage.html].
rows	number	10	The maximum number or rows to return.

Response Parameters

The response will contain either the resulting data table or an error message:

Parameter Name	Value	Notes
columns	[string]	An array of column names.
data	[[string]]	An array of rows, one rank entity per row. Values in each row correspond to the column names in the columns field.
error	string	Only returned if the request failed.

Example

For example, using curl in a shell command:

```
$ curl "https://example.com/flowtraq/api/v1/stat?auth_token=18265a85ca45db35d0a8c263e6dd2c37&group_by=COUNTRY&count_by=BYTES&time_range=15m"
{"columns": ["COUNTRY", "SENT BYTES", "COLORS", "SENT BYTES", "RECV BYTES", "SENT PKTS", "RECV PKTS", "SESS. INIT", "SESS. ACPT", "TIME SERIES"], "data": [{"192.0.0.7", "291953601", "9f5afbfff", "291953601", "288067046", "597183", "592799", "192067046", "2473710", "2478259", ... ] ... ]}
```

Retrieving Raw NetFlow Sessions

Raw NetFlow session records may be retrieved from FlowTraq storage API via:

GET <https://example.com/flowtraq/api/v1/sessions>

Request Parameters

Request parameters are the same as when retrieving processed FlowTraq views. See [Retrieving Processed FlowTraq Views: Request Parameters](#).

Response Parameters

The response will contain either the resulting data table or an error message:

Parameter Name	Value	Notes
columns	[string]	An array of column names.
data	[[string]]	An array of rows, one session per row. Values in each row correspond to the column names in the columns field.
summary	[string]	A total byte and session count of the query.
error	string	Only returned if the request failed.

Example

For example, using curl in a shell command:

```
$ curl "https://example.com/flowtraq/api/v1/sessions?auth_token=18265a85ca45db35d0a8c263e6dd2c37&group_by=COUNTRY&count_by=BYTES&..."
{"columns":["CLIENT ADDRESS","CLIENT COUNTRY","CLIENT AS", ... ],"data":[[{"192.168.68.13","??","0", ... }, ... ], "summary":["Total sessions: 802","Total Packets: 1832127","Total Bytes: 1160933394"]}
```

Appendix D. Flow FAQs

Frequently Asked Questions

1. What is network flow?

Network flow is the equivalent of a 'pen register' for Internet traffic: http://en.wikipedia.org/wiki/Pen_register .

Conceptually, a pen register for Internet traffic is a record of "who communicated with whom; when did they communicate; how much did they communicate; and over what channels did they communicate", without including the actual content of any communications.

2. How is flow analysis useful?

Flow analysis is useful in many ways: it helps pinpoint network bottlenecks, find causes of slowdowns, and see sources of attacks or information leaks, all without doing computationally expensive and privacy issue-raising content analysis.

Also, since the total number of network flows grows very slowly over time in comparison to the growth in bandwidth utilization, flow analysis is scalable far into the future. This is counterintuitive, because the size of each of our communications is growing rapidly. But because network flow is like an Internet pen register, it records when a conversation took place, between whom, what application was used, and how long it took. The actual number of bytes transferred is inconsequential, as none of the actual content bytes are saved.

This means that a flow record for a short and small communication (for instance, a DNS lookup) takes just as much space to store as a large communication (for instance, a streaming video). Longer conversations don't take any more space in a session database!

Over the years, network communications have grown exponentially in volume, but only linearly in count. On average, each network user only produces twice the number of flows than they did two years ago, even though each flow is *eight times as large* on average. This is why flow analysis will scale, while packet captures won't.

3. What are the privacy concerns surrounding flow analysis?

Although it is true that no content is retained in flow analysis, in some cases the source and destination of traffic can still reveal a lot of information by inference.

For instance, suppose flow analysis is used to monitor a network with an 'acceptable use policy' in place. The policy states that employees must not use corporate email for personal reasons. Even though the 'to:' and 'from:' fields in any email communications are not contained in a flow records, one can still tell to which server the connection was made, and that the email protocol (SMTP) was used.

This means that an employee communicating with their spouse who works at 'mysmallbusiness.com' will quickly be found to be in violation of policy, while another employee communicating with a friend at 'gmail.com' won't, since legitimate customers might be using Gmail for their communications.

Keep in mind, however, that in both cases the content of the emails remains private.

4. How can I get started with flow analysis?

Flow reports are generated by devices that either relay traffic (like routers or switches), or devices that can monitor the network for traffic (like sniffers). These devices are called 'exporters.'

Flow analysis, on the other hand, is done by software, running on a server that collects these flow reports from one or more exporters. Such software programs are called 'collectors.' What the collector does with the flow reports often determines the usefulness of the flow analysis tool.

If you want to benefit from flow analysis, you will need both a collector and one or more exporters. Most routers and switches will export network flows in one of the following formats: NetFlow, sFlow, cFlow, or jFlow. However, not all collectors accept all formats. Check your equipment before deciding on a collector.

If you don't have any devices on your network that are capable of exporting network flow, consider using a software flow exporter. This is software agent that can run on any network-attached computer which summarizes the traffic it observes as network flow. We offer a program called Flow Exporter for this purpose. More information on Flow Exporter can be found at <http://www.flowtraq.com/corporate/product/flow-exporter>.

5. How do I select a network flow collector?

The answer to this question depends on what you hope to achieve. Flow collectors are broadly classified in two different categories: aggregators and full-fidelity collectors.

Aggregators periodically generate a pre-configured set of reports on the records they've collected, and store those reports in a database, and discard the records they are holding. They only hold flow records for as long as it takes to generate the pre-configured set of reports. This process is quick and easy, and allows you general insight into network traffic patterns. If you simply want to monitor how busy your network is, an aggregator might work for you.

On the other hand full-fidelity flow collectors store every flow record they receive in a database, and allow you to filter and view the traffic after-the-fact and in much more detail than aggregators. Generally these tools are more computationally expensive, but they offer a much wider range of possibilities. CERT's SiLK is a full-fidelity collector, as is FlowTraq.

If you want to analyze unique traffic patterns and investigate never-before-seen attacks, you will need to invest some time and money in full-fidelity flow collector.

Both aggregators and full fidelity flow collectors are often marketed as using the term "flow analyzer."

Understand the differences and let your operational needs drive your deployment decision!

6. How can I place a software flow exporter most effectively?

Since a software exporter works by sniffing traffic and generating flow summaries based on it, it is only as effective as the traffic it can actually see. This means that a computer located on the edges of your network will most likely see very little of the traffic passing through your organization.

Instead, it is often better to place the software exporter on a network tap or a mirror port (also known as a SPAN port) on a router or switch, allowing it to see all traffic that passes through.

In fact, simply connecting a software exporter to a switch will only allow it to see its own traffic, as switches are smart about what traffic to send to a connected computer, and what to withhold. So you actually must put the switch port in a mirroring mode to allow the software exporter to effectively monitor the traffic on the switch!

Appendix D. Legal Notices

END USER LICENSE AGREEMENT FOR FLOW-TRAQ

This End-User License Agreement (this "Agreement") is a legal agreement between the entity for which you are authorized to enter into this Agreement ("Licensee") and Process Query Systems, LLC ("Licensor") for the Licensor software product identified above (the "Licensed Software"), and the related associated media, printed materials, and "online" or electronic documentation (collectively, the "Documentation"). The Licensed Software also includes any updates, upgrades and supplements to the original Licensed Software provided to Licensee by Licensor, if any.

YOU HEREBY ACKNOWLEDGE AND REPRESENT THAT YOU ARE AUTHORIZED TO ENTER INTO THIS AGREEMENT ON BEHALF OF LICENSEE.

YOU ALSO AGREE THAT LICENSEE'S USE OF THE LICENSED SOFTWARE CONSTITUTES AN ACKNOWLEDGMENT THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT, AND THAT LICENSEE SHALL BE BOUND BY ITS TERMS AND CONDITIONS.

THE LICENSED SOFTWARE IS PROTECTED BY COPYRIGHT LAWS OF THE UNITED STATES AND INTERNATIONAL COPYRIGHT TREATIES, AS WELL AS OTHER INTELLECTUAL PROPERTY LAWS AND TREATIES.

THE LICENSED SOFTWARE IS LICENSED, NOT SOLD.

By clicking on the "I accept the terms of the Licensee Agreement" button, "Accept" button, or similar button, or by installing, copying, downloading, accessing, or otherwise using the Licensed Software, Licensee agrees to be bound by the terms and conditions of this Agreement. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS OF THIS AGREEMENT ON BEHALF OF LICENSEE, OR IF LICENSEE DOES NOT AGREE TO SUCH TERMS, THEN CLICK ON THE "I do NOT accept the terms of the License Agreement" button, "DO NOT ACCEPT" BUTTON, OR SIMILAR BUTTON, AND/OR DO NOT INSTALL OR USE THE LICENSED SOFTWARE.

1.0 LICENSE.

1.1 License Type.

The Licensed Software is licensed to Licensee, pursuant to the terms of this Agreement, on a Subscription License (as defined below) basis, a Perpetual License (as defined below) basis, or an Evaluation License (as defined below) basis. The license key, a series of numbers, letters, and other symbols provided by Licensor, (the "License Key") determines whether Licensee's license is a Subscription License, a Perpetual License, or an Evaluation License, provided that if the License Key does not specify the type of license, then the Licensed Software shall be deemed to be licensed pursuant to a Subscription License and Licensee shall be obligated to pay the applicable license fee. In no event shall this Agreement be interpreted to provide Licensee with more than one type of license. A separate License Key shall be required for each server onto which the Licensed Software is installed.

1.2 Pilot Program.

In the event that Licensor provides the Licensed Software to Licensee in connection with Licensor's Pilot Program (the "Pilot Program") and Licensee has executed and delivered to Licensor the applicable License and Participant Agreement or other license agreement pursuant to which Licensor grants

to Licensee a license to use the Licensed Software in connection with the Pilot Program (the "Pilot Program License Agreement"), then the terms of the Pilot Program License Agreement shall apply to Licensee's use of the Licensed Software in connection with the Pilot Program and the terms of this Agreement shall not apply. If Licensee wishes to use the Licensed Software after expiration of Licensee's participation in the Pilot Program, then Licensee must contact Licensor to purchase a Subscription License or Perpetual License and pay the applicable Subscription Fee or Licensee Fee, as the case may be. Upon Licensor generating (a) a new License Key for a Subscription License and Licensee's payment of the applicable Subscription Fee, then Licensee's license shall thereafter be deemed to be a Subscription License, or (b) a new License Key for a Perpetual License and Licensee's payment of the applicable License Fee, then Licensee's license shall thereafter be deemed to be a Perpetual License.

1.3 Subscription License Grant.

If the License Key provided to Licensee is for a Subscription License, then subject to payment of the applicable subscription fee (the "Subscription Fee") and the terms and conditions of this Agreement, Licensor hereby grants to Licensee and Licensee hereby accepts a limited, non-exclusive right and license (the "Subscription License") to use the Licensed Software and the Documentation during the Initial Term (as defined in Section 2.1(a)) and any Renewal Term (as defined in Section 2.1(c)), for its internal business use only on a single server or other computer.

1.4 Perpetual License Grant.

If the License Key provided to Licensee is for a Perpetual License, then, subject to payment of the applicable license fee (the "License Fee") and the terms and conditions of this Agreement, Licensor hereby grants to Licensee and Licensee hereby accepts a limited, perpetual (except as otherwise set forth herein), non-exclusive right and license (the "Perpetual License") to use the Licensed Software and the Documentation, beginning on the Effective Date (as defined in Section 2.1(a)), for its internal business use only on a single server or other computer.

1.5 Evaluation License Grant.

(a) If the License Key provided to Licensee is for an Evaluation License, then, subject to the terms and conditions of this Agreement, Licensor hereby grants to Licensee and Licensee hereby accepts a limited, temporary, non-exclusive right and license (the "Evaluation License") to use the Licensed Software and the Documentation, beginning on the Effective Date, for evaluation purposes for its internal business use only on a single server or other computer. The duration of the Evaluation License shall be limited to a specific number of days (the "Evaluation License Period"), as determined by the applicable License Key, provided that if the License Key does not specify the number of days, then the Evaluation License Period shall be 120 days.

(b) If Licensee wishes to use the Licensed Software after expiration of the Evaluation License Period, then Licensee must contact Licensor to purchase a Subscription License or Perpetual License and pay the applicable Subscription Fee or Licensee Fee, as the case may be. Upon Licensor generating (i) a new License Key for a Subscription License and Licensee's payment of the applicable Subscription Fee, then Licensee's license shall thereafter be deemed to be a Subscription License, or (ii) a new License Key for a Perpetual License and Licensee's payment of the applicable License Fee, then Licensee's license shall thereafter be deemed to be a Perpetual License.

(c) The following provisions of this Agreement shall be deemed to be modified as follows during the Evaluation License Period:

(i) Licensor provides no warranty, express or implied, of any kind during the Evaluation License Period. During the Evaluation License Period, Licensor provides the Licensed Software "AS IS", AND THE LIMITED WARRANTY (AS DEFINED IN SECTION 5.1) SHALL NOT APPLY, AND SHALL BE VOID AND OF NO FORCE AND EFFECT.

(ii) During the Evaluation License Period, the indemnification provisions of Article 7.0 shall be void and of no force and effect, and Licensors shall have no indemnification obligations pursuant to this Agreement.

(iii) During the Evaluation License Period, Licensors shall provide the Maintenance Services (as defined in Section 4.1) and Support Services (as defined in Section 4.4) only on a limited, as-available basis.

Evaluation License - Certain Restrictions.

(a) If Licensee uses the Licensed Software pursuant to an Evaluation License, then the provisions of this Section shall apply.

(b) Notwithstanding the presence or absence of any copyright and/or proprietary legends in the Licensed Software, Licensee agrees to keep confidential all information concerning the Licensed Software received from Licensors or otherwise obtained by Licensee, during the term of this Agreement, and not to disclose any information concerning the Licensed Software to any third party without Licensors' prior written approval. Licensee shall permit access to the Licensed Software only to those employees of Licensee that are involved in testing and evaluating the Licensed Software. Licensee agrees to inform each of its employees given access to the Licensed Software or any portion thereof of the confidential nature thereof and to require them to abide by Licensee's obligations under this Agreement. Licensee shall not be required to maintain the confidentiality of information to the extent that Licensee can demonstrate that such information is or becomes known to the public from a source other than through Licensee without breach of a confidentiality restriction.

(c) All reports, designs, specifications, and other materials and all rights in all media made and/or developed which pertain to the Licensed Software, whether prepared by Licensors or Licensee, shall be the exclusive property of Licensors throughout the world; and all such reports, designs, specifications or other materials and all media shall be kept confidential by Licensee. In addition, Licensors shall have the sole and exclusive right to register copyright of such materials in its own name in any and all countries and to obtain renewals and manufacture, reproduce, publish, distribute, and sell such media. All right, title, and interest throughout the world to any invention relating to enhancement of the Licensed Software, whether or not patentable, conceived in or made in the course of or as a result of Licensee's efforts shall be the exclusive property of Licensors. Licensee agrees to assign and hereby does assign all right, title and interest in and to any such media, reports, designs, specifications or other materials, or inventions to Licensors, and Licensee agrees to perform all acts and execute all applications, assignments and other documents reasonably necessary or desirable to effectuate the foregoing assignment.

(d) Licensee covenants and agrees that:

(i) the Licensed Software will be installed only at the one (1) site owned by Licensee;

(ii) the Licensed Software will only be accessed by employees of Licensee;

(iii) the Licensed Software will not be used for any purpose other than internal evaluation and, specifically, will not be used in or for Licensee's actual business operations;

(iv) Licensee shall provide a suitable and adequate computing environment (including appropriate hardware) for the installation, use and evaluation of the Licensed Software;

(v) Licensee shall provide Licensors with status reports and other information relating to Licensee's use of Licensed Software as may be reasonably requested from time to time by Licensors; and

(vi) Licensee agrees that during and after the Evaluation License Period, Licensee will not make any announcement or otherwise make public any assessment or feedback of the Licensed Software without the prior written consent of Licensors.

1.7 Licensed Copy(ies).

Licensee may install and use one (1) copy of the Licensed Software on a single operating system on a single computer for each licensed copy of the Licensed Software licensed by Licensee. Only the number of concurrent users for which Licensee has purchased a license may use such copy of the Licensed Software.

1.8 Licensee Changes.

(a) At any time during the term of this Agreement, at Licensee's request, and subject to Licensee being in compliance with its obligations under this Agreement, and payment of additional License Fees (with respect to a Perpetual License) or Subscription Fees (with respect to a Subscription License), Licensors agrees to provide to Licensee license keys to authorize use of the Licensed Software on one (1) or more additional servers (each an "Authorized Server"). In the event of any such increase, the License Fee (and applicable Maintenance Service Fees (as defined in Section 4.3)) or Subscription Fee payable by Licensee under this Agreement shall be adjusted accordingly, based on the then applicable Subscription Fee or License Fee (and Maintenance Service Fee) for the total number of Authorized Servers. With respect to a Subscription License, the Subscription Fees payable by Licensee for the year in which such increase in Authorized Servers takes effect shall be prorated according to the number of full or partial months remaining in the year in which such increase takes effect.

(b) In the event that Licensee wishes to reduce the number of Authorized Servers under the Perpetual License during the term of this Agreement, Licensee shall provide written notice to Licensors of such reduction. Licensee shall be responsible for payment of the full amount of the Maintenance Services Fee for the entire Maintenance Period (as defined in Section 4.3), in which the reduction occurs. In addition, all License Fees and Maintenance Service Fees are NON-REFUNDABLE and Licensee shall not receive any refund for any License Fees or for any portion of the Maintenance Service Fees as a result of a reduction in the number of Authorized Servers.

(c) Licensee may not reduce the number of Authorized Servers under the Subscription License during the Initial Term or any Renewal Term. However, Licensee shall have the right to reduce the number of total Authorized Servers effective as of the first day of any Renewal Term by providing Licensors with notice of such change. With respect to a Subscription License, in the event of any reduction in the number of Authorized Servers pursuant to the terms of this Agreement, the Subscription Fees payable by Licensee for the applicable Renewal Term shall be adjusted accordingly.

1.9 Licensee Hardware Requirements. Licensee shall provide a suitable and adequate computing environment (including appropriate hardware) for the installation and use of the Licensed Software, and hereby acknowledges and agrees that the failure to provide such a computing environment may adversely affect the ability of the Licensed Software to function fully.

2.0 TERM AND TERMINATION.

2.1 Term; Initial Term and Renewal Terms.

(a) If Licensee purchases a Subscription License, then the initial term of the Subscription License (the "Initial Term") shall be the one (1) year period commencing on the day on which Licensors generates the applicable License Key (the "Effective Date").

(b) If Licensee purchases a Perpetual License, then the term of the Perpetual License shall commence on the Effective Date and continue thereafter until terminated in accordance with the provisions of this Agreement.

(c) If Licensee purchases a Subscription License, then Licensee may extend the term of the Subscription License beyond the Initial Term for one (1) or more additional one (1) year periods (each, a "Renewal Term") provided that Licensee provides Licensors with written notice of renewal (the "Renewal Notice") prior to the expiration of the then current Initial Term or Renewal Term, and pays to Licensors the then applicable Subscription Fees prior to the expiration of the then current Initial Term or Renewal

Term. The Subscription Fees payable for any Renewal Term shall be at Licensor's annual subscription rates then in effect on the date of the Renewal Notice.

(d) The term of this Agreement shall commence on the Effective Date and shall continue thereafter until terminated in accordance with the provisions of this Agreement.

2.2 Termination for Non-Payment.

(a) Any amount payable to Licensor hereunder (including any License Fee, Subscription Fee, Maintenance Service Fee, or Support Service Fee) which is overdue shall accrue interest at the rate of one percent (1%) per month until paid in full.

(b) In addition, in the event that Licensee fails to pay within thirty (30) days after the applicable due date any License Fee, Subscription Fee, Maintenance Fee, or Support Service Fee, then (i) with respect to any unpaid License Fee, Licensor may immediately terminate the applicable Perpetual License by sending written notice of termination to Licensee, and (ii) with respect to any unpaid Subscription Fee, Licensor may immediately terminate the applicable Subscription License and terminate providing any Maintenance Services by sending written notice of termination or suspension to Licensee, (iii) with respect to any unpaid Maintenance Fee, Licensor may immediately suspend providing any Maintenance Services without notice, or immediately terminate providing any Maintenance Services by sending written notice of termination, and (iv) with respect to any unpaid Support Service Fee, Licensor may immediately suspend providing any Support Services without notice, or immediately terminate providing any Support Services by sending written notice of termination.

2.3 Termination By Either Party.

(a) Licensee may terminate this Agreement at any time by notifying Licensor in writing of termination. Upon termination of this Agreement by Licensee, the Evaluation License, Subscription License or Perpetual License (as the case may be) shall also automatically and immediately terminate. All fees paid by Licensee, including all License Fees, Subscription Fees, Maintenance Fees, and Support Services Fees, are NON-REFUNDABLE.

(b) In addition to the provisions of Section 2.2 above and without prejudice to any other rights, Licensor may terminate this Agreement by written notice to Licensee if Licensee breaches or otherwise fails to comply with the terms and conditions of this Agreement. Upon any such termination of this Agreement by Licensor, the Evaluation License, Subscription License or Perpetual License (as the case may be) shall also automatically and immediately terminate.

2.4 Effect of Termination.

(a) Upon any termination of the Evaluation License, Subscription License (but not upon expiration of the Initial Term or Renewal Term pursuant to Section 2.1(c)) or the Perpetual License (as the case may be), Licensee shall immediately discontinue use of the Licensed Software and shall within three (3) days return to Licensor, or certify destruction of, all full or partial copies of the Licensed Software and Documentation.

(b) No termination of the Subscription License, the Perpetual License, or this Agreement shall (i) relieve Licensee from its obligation to pay any charges for Subscription Fees, Licensee Fees, or fees for Maintenance Services or Support Services accrued prior to the termination date, or (ii) except as specifically set forth in Section 5.3, obligate Licensor to refund or otherwise return any payments made by Licensee pursuant to this Agreement. ALL LICENSE FEES, SUBSCRIPTION FEES, MAINTENANCE FEES, AND SUPPORT SERVICES FEES PAID TO LICENSOR ARE NON-REFUNDABLE.

(c) The provisions of Sections 1.5(c)(i), 1.5(c)(ii), 1.6(b), 1.6(c), 2.2(a), 2.4, 3.5, 3.8, 5.2, 5.3, 6.1, 6.2, 8.1, 8.2, 8.3, 8.4, and of Article 9.0 shall survive termination of this Agreement.

3.0 OTHER RIGHTS AND LIMITATIONS.

3.1 Limitations on Reverse Engineering, Decompilation, and Disassembly.

Licensee may not reverse engineer, decompile, or disassemble the Licensed Software, except to the extent that this restriction is expressly prohibited by law.

3.2 Separation of Components.

The Licensed Software is licensed as a single product. Its component parts may not be separated by Licensee for any reason.

3.3 Limited Copy Rights.

During the term of the Subscription License (if Licensee purchases a Subscription License) or the Perpetual License (if Licensee purchases a Perpetual License), and subject to the inclusion of any and all copyright and proprietary notices appearing in or on the Licensed Software in the form provided by Licensor, Licensee may make a reasonable number of copies of the Licensed Software, but only as may be necessary for archival, back-up, or disaster recovery purposes. Licensee may not make any copies of the Licensed Software used pursuant to an Evaluation License.

3.4 Restrictions on Transfer.

Licensee may not rent, lease, sell, sublicense, distribute, or otherwise transfer (including, without limitation, transfer by operation of law in connection with a merger) rights to the Licensed Software unless Licensee obtains Licensor's prior, express written consent.

3.5 Intellectual Property Rights.

(a) The Licensed Software and the Documentation, as well as all patents, copyrights, trademarks, service marks, trade secrets, and other intellectual property and proprietary rights in or related to the Licensed Software and the Documentation (collectively, the "IP Rights"), are and will remain the exclusive property of Licensor or its licensors, whether or not specifically recognized or perfected under the laws of the jurisdiction in which the Licensed Software is used or licensed. Licensee shall not take any action that jeopardizes any of the IP Rights. Except for the specific license rights granted to Licensee pursuant to this Agreement, Licensee shall not have or acquire under this Agreement any right, title, or interest in or to the Licensed Software or the Documentation.

(b) Without limiting the generality of the provisions in subsection (a) above, this Agreement does not grant Licensee any rights in connection with any trademarks or service marks of Licensor.

3.6 Geographical Limitations.

The Licensed Software and the Documentation may only be used in the United States and in any country that is a party to the Berne Copyright Convention, subject, however, to compliance with applicable U.S. export laws and regulations. Licensee shall be responsible, at its expense, for complying with all applicable laws and regulations of each jurisdiction where there is a user of the Licensed Software (including, without limitation, laws and regulations pertaining to (a) exports or imports of software and related property, (b) use or remote use of software and related property, and (c) registration of this Agreement). Licensee shall indemnify and hold harmless Licensor and its affiliates from and against all actions, claims, and proceedings brought or asserted against, and all damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) suffered or incurred, by Licensor and its affiliates arising out of any violation or alleged violation by Licensee of any such laws or regulations.

3.7 Export Compliance.

The Licensed Software may contain strong encryption and may be subject to United States export controls. Licensee shall not export or re-export the Licensed Software, directly or indirectly, in violation of applicable export restrictions, including to:

- (a) any countries that are subject to United States export restrictions;
- (b) any end-user who Licensee knows or reasonably should know will utilize them in the design, development or production of military, nuclear, chemical or biological weapons; or
- (c) any end-user who has been prohibited from participating in the United States export transactions by any federal agency of the United States government.

Licensee further acknowledges that the Licensed Software may include technical data subject to export and re-export restrictions imposed by United States law, and Licensee shall comply with all such applicable United States laws.

3.8 Audit Rights.

At Licensors request from time to time, Licensee shall provide Licensor with a list of all copies and locations of the Licensed Software and the Documentation. Licensor, or an auditor of Licensor's choosing, may also from time to time perform an audit of Licensee's use of the Licensed Software and the Documentation and Licensee's compliance with the terms of this Agreement. Any such audit shall be made during Licensee's normal business hours, shall be undertaken after reasonable prior written notice thereof has been given by Licensor to Licensee, and shall not unreasonably interfere with Licensee's business operations. Licensee agrees to cooperate with Licensor in any such audit. In the event that any such audit indicates a deployment of the Licensed Software in excess of the specified number of Authorized Servers, Licensee shall promptly reimburse Licensor for the costs of such audit and pay additional Subscription Fees or Licensee Fees (as the case may be) to Licensor for such unauthorized use.

4.0 MAINTENANCE AND SUPPORT SERVICES

4.1 In General - Maintenance Services.

Licensor shall provide Licensee with those maintenance services for the Licensed Software set forth below ("Maintenance Services") in accordance with the terms of this Agreement. Such Maintenance Services shall include (a) all new releases, corrections, bug fixes, enhancements, updates, and other changes (but generally excluding new software modules) to the Licensed Software as Licensor generally releases to its other customers who have contracted for Maintenance Services for the Licensed Software, and (b) access to Licensor's maintenance and support center on the World Wide Web. Licensee may request Maintenance Services by sending an email to "support@proquesys.com", and in the event that a particular matter is not resolved by the online maintenance and support center or by email in a reasonable period of time, Licensee may request telephone support from 9:00 a.m. until 5:00 p.m. (Eastern Time) each business day.

4.2 Maintenance Services - Subscription License.

If Licensee purchases a Subscription License, then the cost of the Maintenance Services is included in the Subscription Fee. Licensor shall provide Maintenance Services during the Initial Term and any Renewal Term for which the Subscription Fee is paid in full. Maintenance Services will end immediately and automatically upon expiration of the Initial Term or Renewal Term pursuant to Section 2.3, or termination of the Subscription License or this Agreement.

4.3 Maintenance Services - Perpetual License.

(a) If Licensee purchases a Perpetual License, then the License Fee does not include the cost of Maintenance Services. Instead, Licensee must pay an additional fee for Maintenance Services (the "Maintenance Services Fee") for each year of the term of this Agreement for which Licensee desires Maintenance Services (the "Maintenance Period"). The fee for Maintenance Services must be paid in full in advance for each such year.

(b) If Licensee purchases a Perpetual License, then Licensee is not required to purchase Maintenance Services for periods after the Initial Term. However, if Licensee does not purchase Maintenance Services for some period of time, and thereafter purchases Maintenance Services, then, in addition to the Maintenance Fees otherwise payable to Licensor, Licensee shall also pay the full amount of all Maintenance Fees that would have been payable by Licensee had Licensee purchased such Maintenance Services at Licensor's standard rates for all prior periods in which Licensee did not pay Licensee for such Maintenance Services.

4.4 Support Services.

(a) "Support Services" means any services provided by Licensor with respect to the Licensed Software, other than the Maintenance Services, and may include (i) assisting Licensee with optimizing Licensee's use of the Licensed Software, (ii) consulting with Licensee regarding the functionality and capabilities of the Licensed Software, (iii) assisting Licensee with use of the Licensed Software (including the building of filters, views, or workspaces) to achieve Licensee's particular goals, or (iv) advising Licensee regarding the strategic deployment of the Licensed Software through Licensee's entire enterprise.

(b) Neither the Subscription Fee nor the License Fee includes fees for providing Support Services, and Licensee shall pay Licensor a separate fee for providing the Support Services (the "Support Services Fee").

4.5 Licensee-Provided Information.

With respect to technical information Licensee provides to Licensor in connection with the Maintenance Services or Support Services, Licensor may use such information for its business purposes, including for product maintenance, support and development. Licensor will not utilize such technical information in a form that identifies Licensee.

5.0 WARRANTY PROVISIONS

5.1 Limited Warranty.

Licensor warrants that, for a period of thirty (30) days from the date on which the Licensed Software is delivered to Licensee, by download, on a physical media, or otherwise (the "Limited Warranty Period"), the Licensed Software will perform substantially in accordance with the Documentation (the "Limited Warranty"). HOWEVER, LICENSOR DOES NOT WARRANT THAT LICENSEE'S USE OF THE SOFTWARE WILL BE UNINTERRUPTED OR THAT THE OPERATION OF THE SOFTWARE WILL BE ERROR-FREE.

5.2 Limitations.

(a) The Limited Warranty shall immediately terminate if (i) any modifications are made to the Licensed Software by Licensee or any third party (other than a third party authorized by Licensor to make specific modifications) during the Limited Warranty Period, (ii) the media (if any) on which the Licensed Software is delivered is subjected to accident, abuse, or improper use, or (iii) Licensee breaches the terms of this Agreement.

(b) The Limited Warranty shall not apply if the Software is used on or in conjunction with hardware or software other than the unmodified version of hardware and software with which the Software was designed to be used as described in the Documentation. THE LIMITED WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS; LICENSEE MAY HAVE OTHER RIGHTS THAT VARY FROM STATE/JURISDICTION TO STATE/JURISDICTION.

(c) The Limited Warranty shall not apply unless Licensee informs Licensor of the problem with the Licensed Software during the Limited Warranty Period.

(d) THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT ARE IN LIEU OF, AND LICENSOR DISCLAIMS, ANY AND ALL OTHER WARRANTIES, CONDITIONS, OR REPRESENTATIONS (EXPRESS OR IMPLIED, ORAL OR WRITTEN), WITH RESPECT TO THE LICENSED SOFTWARE OR ANY PART THEREOF OR WITH RESPECT TO ANY SERVICES PROVIDED OR TO BE PROVIDED BY LICENSOR, WHETHER ALLEGED TO ARISE BY LAW, BY REASON OF CUSTOM OR USAGE IN THE TRADE, BY COURSE OF DEALING, OR OTHERWISE. SUCH DISCLAIMED WARRANTIES INCLUDE, BUT ARE NOT LIMITED TO, ANY AND ALL IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS OR SUITABILITY FOR ANY PURPOSE (WHETHER OR NOT LICENSOR KNOWS, HAS REASON TO KNOW, HAS BEEN ADVISED, OR IS OTHERWISE IN FACT AWARE OF ANY SUCH PURPOSE), OR NON-INFRINGEMENT. THE WARRANTIES SET FORTH IN THIS AGREEMENT ARE MADE SOLELY TO LICENSEE AND NOT TO OR FOR THE BENEFIT OF ANY THIRD PARTY.

5.3 Remedies.

Licensor's sole liability for a breach of the Limited Warranty, and Licensee's sole remedy, shall be (in Licensor's sole discretion): (a) to replace the defective media on which the Licensed Software was delivered; (b) to advise Licensee how to achieve substantially the same functionality with the Licensed Software as described in the Documentation through a procedure different from that set forth in the Documentation; or (c) if the above remedies are impracticable in Licensor's judgment, to refund the Subscription Fee or License Fee (as the case may be) Licensee paid for the Licensed Software and terminate this Agreement and the Subscription License or Perpetual License (as the case may be). Repaired, corrected, or replaced Licensed Software shall be covered by the Limited Warranty for the longer of (a) the unexpired portion of the then applicable Limited Warranty Period, or (b) thirty (30) days after the date Licensor either shipped to Licensee the repaired or replaced Licensed Software or advised Licensee as to how to operate the Licensed Software so as to achieve the functionality described in the Documentation, whichever is applicable.

6.0 LIMITATION OF LIABILITY

6.1 Consequential Damages Limitation.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL LICENSOR BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE, OR CONSEQUENTIAL LOSSES OR DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, COMPUTER FAILURE OR MALFUNCTION OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF OR RESULTING FROM THE USE OF OR INABILITY TO USE THE LICENSED SOFTWARE, THE MAINTENANCE SERVICES, OR THE SUPPORT SERVICES, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE PROVISIONS OF THIS SECTION SHALL NOT APPLY TO A BREACH BY LICENSOR OF ITS OBLIGATIONS UNDER ARTICLE 7.0 OR A CLAIM FOR PERSONAL INJURY OR PROPERTY DAMAGE (EXCLUDING, HOWEVER, ANY SUCH CLAIM AGAINST LICENSOR RELATING TO THE PERFORMANCE OR NON-PERFORMANCE OF THE LICENSED SOFTWARE OR ANY OF LICENSOR'S SERVICES).

6.2 Direct Damages Limitation.

LICENSOR'S LIABILITY FOR ANY BREACH OR DEFAULT UNDER THIS AGREEMENT (INCLUDING, WITHOUT LIMITATION, ANY BREACH OF ANY WARRANTY GIVEN BY LICENSOR UNDER THIS AGREEMENT) SHALL BE LIMITED TO THE AMOUNT OF LICENSEE'S DIRECT DAMAGES RESULTING FROM SUCH BREACH OR DEFAULT, NOT TO EXCEED THE AMOUNTS RECEIVED BY LICENSOR WITH RESPECT TO THE LICENSED SOFTWARE, THE MAINTENANCE SERVICES, OR SUPPORT SERVICES GIVING

RISE TO SUCH BREACH OR DEFAULT, IN THE ONE (1) YEAR PERIOD IMMEDIATELY PRECEDING THE DATE ON WHICH THE CAUSE OF ACTION ACCRUED. THE PROVISIONS OF THIS SECTION SHALL NOT APPLY TO AMOUNTS PAYABLE BY LICENSOR TO A THIRD PARTY CLAIMANT UNDER ARTICLE 7.0 OR A CLAIM FOR PERSONAL INJURY OR PROPERTY DAMAGE (EXCLUDING, HOWEVER, ANY CLAIM AGAINST LICENSOR RELATING TO THE PERFORMANCE OR NON-PERFORMANCE OF THE LICENSED SOFTWARE OR ANY OF LICENSOR'S SERVICES).

7.0 INDEMNIFICATION

7.1 Third-Party Claims.

Licensor will defend at its own expense any action against Licensee brought by a third party to the extent that the action is based upon a claim that the Licensed Software infringes any United States copyright or misappropriates any United States trade secret, and Licensor will pay those costs and damages finally awarded against Licensee in any such action that are specifically attributable to such claim or those costs and damages agreed to in a monetary settlement of such action made by Licensor.

7.2 Conditions.

Licensor's obligations under Section 7.1 are conditioned on (a) Licensee notifying Licensor promptly in writing of the commencement of any such action, (b) Licensee giving Licensor sole control of the defense thereof and any related settlement negotiations, and (c) Licensee cooperating with Licensor in such defense.

7.3 Licensor's Options.

If the Licensed Software becomes, or in Licensor's opinion is likely to become, the subject of an infringement or misappropriation claim, Licensor may, at its option and expense, either (a) procure for Licensee the right to continue using the Licensed Software, (b) replace or modify the Licensed Software so that it becomes non-infringing, or (c) terminate the Evaluation License, Subscription License or Perpetual License, as the case may be. If the License is terminated under clause (c) above, then Licensor shall refund to Licensee the following amount: (i) with respect to a Subscription License, a portion of the annual Subscription Fee pro-rated according to the remaining portion of the then current Initial Term or Renewal Term, and (ii) with respect to a Perpetual License, a pro rata portion of the Licensee Fee, amortized over the first five (5) year period of the Perpetual License.

7.4 Exclusions.

Notwithstanding the foregoing, Licensor will have no obligation with respect to any infringement or misappropriation claim if the Licensed Software (a) is being used not in accordance with this Agreement or not in accordance with the Documentation, or (b) has been modified by Licensee or any third party.

7.5 Entire Liability.

Licensor's obligations under this Article shall constitute its only obligations in the event that any claim or action is brought against Licensee alleging that the Licensed Software infringes, misappropriates, or otherwise violates the rights of any third party.

8.0 ARBITRATION AND JURISDICTION

8.1 Binding Arbitration.

Licensee and Licensor agree that the exclusive remedy for all disputes and claims relating in any way to, or arising out of, this Agreement (including the arbitrability of any claim or dispute and the enforceability of this paragraph), or to any other alleged act or omission by either party toward the other (excepting only any cause of action giving rise to a claim for equitable relief), shall be binding arbitration.

Any such claim shall be submitted to arbitration before a single arbitrator; provided that if Licensee and Licensor are unable to agree to an arbitrator, the dispute shall instead be submitted to a panel of three (3) arbitrators. The arbitrator(s) shall be selected in accordance with the then-prevailing Rules of Commercial Arbitration of the American Arbitration Association ("AAA"), and the arbitration proceedings shall be conducted in Manchester, New Hampshire.

8.2 Authority of the Arbitrators.

The arbitrator(s) shall not contravene or vary in any respect any of the terms or provisions of this Agreement. The award of the arbitrator(s) shall be final and binding upon Licensor and Licensee, and judgment upon any award rendered therein may be entered and enforced in any court of competent jurisdiction, including the New Hampshire Superior Court.

8.3 Injunctive Relief.

Neither this arbitration provision nor a pending arbitration shall prevent either party from obtaining injunctive relief for any matter at any time.

8.4 Choice of Law.

This Agreement shall be governed by the laws of the State of New Hampshire, without regard to conflicts of law provisions.

9.0 MISCELLANEOUS

9.1 Entire Agreement.

This Agreement shall constitute the complete and exclusive agreement between Licensor and Licensee with respect to the subject matter hereof, and supersedes all prior or contemporaneous communications, proposals, understandings, or other agreements, whether oral, electronic, or written, between them regarding the subject matter hereof. The acceptance of any purchase order by Licensor is expressly made conditional on Licensee's consent to the terms set forth herein.

9.2 Modification.

The terms and conditions contained in this Agreement may not be modified by Licensee except in a writing duly signed by Licensee and an authorized representative of Licensor.

9.3 Notice.

Any notice required to be given to a party under this Agreement shall be in writing and shall be (a) given by personal delivery to such party, (b) mailed by registered or certified mail, return receipt requested, postage prepaid, or (c) shipped by a nationally-recognized overnight carrier, shipping prepaid. Any such notice shall be sent to Licensor at the address set forth below in Article 10.0, or Licensee at the address in Licensor's records. Either party may at any time change the address to which written notices are to be sent to such party, by notifying the other party of the new address by written notice.

9.4 Assignment.

(a) This Agreement shall be binding upon and for the benefit of the parties hereto and their respective successors and permitted assigns. Licensor may assign this Agreement at its discretion. Except as set forth in subsection (b) below, Licensee may not assign, sublicense or otherwise transfer any rights by operation of law or otherwise (including as the result of a merger, sale of assets, stock sale, or other transaction resulting in a change of control) under this Agreement, any license granted hereunder, or any of Licensee's rights hereunder, in whole or in part.

(b) Licensee may assign or transfer this Agreement in its entirety to a purchaser which acquires control of Licensee or all or substantially all of Licensee's assets, but if and only if, (i) no later than thirty

(30) days following such purchase, Licensee and such purchaser provide Licensor with written notice thereof, including the unconditional written agreement by such purchaser to be bound by all of the provisions of this Agreement, and (ii) Licensor consents to such assignment, which consent shall not be unreasonably withheld.

9.5 Severability.

Each term, condition, and provision of this Agreement shall be valid and enforced to the fullest extent permitted by law. If there is any conflict between any term, condition, or provision of this Agreement and any statute, law, ordinance, order, rule, or regulation, the latter shall prevail; provided, that any such conflicting term, condition, or provision shall be curtailed and limited only to the extent necessary to bring it within the legal requirements and the remainder of this Agreement shall not be affected thereby.

9.6 U.N. Convention.

This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is hereby expressly excluded.

9.7 Taxes.

Any United States (whether federal, state, or local) or foreign sales, use, or other taxes (excluding only any tax based on Licensor's net income), assessments, or other governmental fees or charges arising from any payments made or to be made by Licensee to Licensor for the Licensed Software or with respect to its use, or otherwise related to or arising out of this Agreement, are the responsibility of and shall be paid by Licensee or, if Licensor is required to pay the same, shall be reimbursed by Licensee to Licensor upon demand.

9.8 Waiver.

No failure or delay by either party to exercise any right or remedy specified herein shall be construed as a current or future waiver of such remedy or right, unless said waiver is in writing signed by a duly authorized representative of the party issuing such waiver.

10.0 CONTACT INFORMATION

If Licensee has any questions concerning this Agreement, or if Licensee wishes to contact Licensor for any reason, please contact Licensor at the street address or email address below:

Process Query Systems, LLC
16 Cavendish Court
Lebanon, New Hampshire 03766
<support@flowtraq.com>

Third-Party Software Components

Restlet

FlowTraq incorporates Restlet, 2005-2011 Noelios Technologies. "Restlet" is a registered trademark of Noelios Technologies. Restlet is available under the terms of the LGPL 2.1.

For a copy of the Restlet source code, please contact <support@flowtraq.com> or visit <http://www.restlet.org> for the most recent version.

JFreeChart

FlowTraq incorporates JFreeChart, 2000-2009 by Object Refinery Limited and Contributors. JFreeChart is available under the terms of the LGPL 2.1.

For a copy of the JFreeChart source code, please contact <support@flowtraq.com> or visit <http://www.jfree.org> for the most recent version.